Biometrische Identitäten und ihre Rolle in den Diskursen um Sicherheit und Grenzen

Eine Tagungsdokumentation

Biometrische Identitäten und ihre Rolle in den Diskursen um Sicherheit und Grenzen

Dokumentation der gleichnamigen Tagung am 30. November und 1. Dezember 2012

Redaktion: Andrea Knaut, Christian Ricardo Kühne

Satz: Andrea Knaut

Umschlagbild: »Passkontrolle«, Katharina Greve,
http://www.freizeitdenker.de
Mit freundlicher Genehmigung der Künstlerin.

Bildlizenz: Das Bild unterliegt nicht der unten angegebenen CC-Lizenz. Nutzung nur mit Genehmigung der Künstlerin.

Herausgeberin: Andrea Knaut,
Arbeitsgruppe Informatik in Bildung und Gesellschaft,
Institut für Informatik, Humboldt-Universität zu Berlin.
Mit freundlicher Unterstützung durch die
Alcatel-Lucent-Stiftung.

Alcatel-Lucent Stiftung für Kommunikationsforschung

INFORMATIK IN BILDUNG & GESELLSCHAFT

HUMBOLDT-UNIVERSITÄT ZU BERLIN

erschienen: August 2013

Inhaltsverzeichnis

Vorbemerkung 1

Identität ist Spurensuche 3
Herbert Hrachovec

»How to liquefy a moving body: Eurodac und die Digitalisierung der Europäischen Grenze« 19
Brigitta Kuster & Vassilis S. Tsianos

Transparenz und Datensparsamkeit von elektronischen Ausweisdokumenten in Deutschland 37
Dominik Oepen

Biometrische Identitäten und ihre Rolle in den Diskursen um Sicherheit und Grenzen 61
Andrea Knaut

Vorbemerkung

»Identitätstechnologien«, in denen der Körper als Schlüssel gilt, sind Teil weltweiter Ausweissysteme. Sie nutzen die automatisierte Personenerkennung, die Biometrie. Die Ideen und »innovativen Lösungen« der neuen Pass-Systeme sind einerseits bereits mehr als zweihundert Jahre alt. Andererseits verändern sie durch ihre Einbettung in vernetzte Rechensysteme bisherige Instrumente zur Bewegungs- und Zugangskontrolle signifikant. Auf welche Weise, mit welchen gesellschaftlichen Konsequenzen dies geschieht und welche historischen Entwicklungen dem zugrundeliegen, lässt sich nur aus mehreren, voneinander verschiedenen analytischen Blickwinkeln erfassen. Wir haben auf der Tagung über biometrische Identitäten am Informatik-Institut der Berliner Humboldt-Universität einige versammelt.

Die vorliegende Veröffentlichung dokumentiert ausgewählte Vorträge. Der erste Text von Herbert Hrachovec ist grundlegender philosophischer Natur. Er verdeutlicht die Tragweite des allzu leichtfertig benutzten Begriffs der Identität und seine eigentümliche Verwendung in der Biometrie. Es folgt ein Vortragsmanuskript zweier Migrationsforscher_innen, in dem die Verschmelzung von Körper und territorialer Grenze soziologisch am Beispiel eines Fingerabdruckidentifizierungssystems für Asylsuchende in der EU untersucht wird. Danach findet sich mit dem Transkript des Vortrags von Dominik Oepen eine vor allem technische Perspektive. Der Text

bietet einen Einblick in die in derzeit genutzten Passdokumenten umgesetzten Datenschutzkonzepte und deren Grenzen.

Thematisch wie stilistisch zeigen sich komplett andere Herangehensweisen an das Tagungsthema. Einen Überblick über die vollständige Bandbreite der Perspektiven aus Philosophie, Rechtsgeschichte, Informatik, Soziologie oder Politikwissenschaft bietet das kritische Protokoll der Tagung am Schluss dieses kleinen Bandes, das alle zwölf Vorträge kommentiert zusammenfasst. Die Kontroverse ist nun der nächste Schritt.

Weitere Audio-Mitschnitte und Vortragsfolien zur Tagung sind verfügbar unter:
http://waste.informatik.hu-berlin.de/tagungen/digiID

Editorische Notiz

Zitierstile und die Wahl des Generis personenbezeichnender Substantive sind in der von den Autor_innen jeweils gewählten Form belassen worden.

Identität ist Spurensuche

Herbert Hrachovec

Mit „Identität“ ist es wie mit „Unterhaltung“ oder „Partnerschaft“: der Ausdruck wird in mehreren, nur lose miteinander verbundenen, Zusammenhängen verwendet. Assoziationen, die sich in einem Fall ergeben, greifen dadurch bisweilen auf sachlich fremde Bereiche über. Die Partnerschaft zwischen Städten hat in mehreren Punkten nichts mit einer Lebenspartnerschaft zu tun. Im Fall von „Identität“ sind – um nur einige zu nennen – die Logik, die Ontologie, die philosophische Psychologie, die Soziologie, Messtheorie und Kriminalistik beteiligt. Im Folgenden wird versucht, charakteristische Eigenheiten des Identitätsbegriffs in ausgewählten Anwendungsgebieten zu markieren und aus diesen Faktoren eine Orientierung für Diskussionen in der Biometrie zusammenzustellen. Identität ist ein Grundzug unseres Weltbezugs und gilt für Sprachausdrücke und Personen; dieser Zusammenhang wird eingangs erläutert. Die Identifizierung erwünschter Messgrößen gehört in einen ganz verschiedenen Kontext, dessen Gesetzlichkeit sich jedoch, zweitens, wenn es darum geht, Personen dingfest zu machen, mit dem ersten Themenfeld überschneidet. Das Verhältnis zwischen der Feststellung einer Variable und der menschlichen Lebensform, die von semi-stabilen Identitätzuschreibungen getragen wird, bildet den Schnittpunkt der beiden Begriffsverwendungen und wird abschließend diskutiert.

Identität

Ein Schlaglicht auf Identität im Umgang mit Sprache liefern die aktuellen Plagiatsdebatten. In ihnen wird deutlich, dass das Interesse an eindeutiger Gleichheit nicht losgelöst von sachspezifischen Umgebungsbedingungen wirksam wird. Gleichlautende Textpassagen erregen kein Aufsehen, wenn sie im Rahmen alltäglicher Kommunikation »handelsüblich« sind, oder wenn eine von ihnen als Zitat gekennzeichnet ist. Eine Unregelmäßigkeit ist die Verletzung der Zitierpflicht, welche den genetischen Zusammenhang der identischen Passagen unterdrückt. Eine Stufe komplizierter ist die nicht-triviale, unausgewiesene Paraphrase. Ein Beispiel aus dem Blog zur Dissertation Annette Schavans.[1] Heinz Häfner schreibt

> »In der Weiterführung der evolutionistischen Tradition Darwins […] hat Freud auf der Basis therapeutischer Erfahrungen als Nervenarzt ein genetisch-psychodynamisches Modell des Gewissens entwickelt. Er ging von der Beobachtung aus, daß Schuldgefühle, ähnlich wie die Angst, einer der stärksten dynamischen Faktoren psychischer Störungen in unserer Kultur sind […].«[2]

Dem steht folgende Passage aus Frau Schavans Dissertation gegenüber:

> »Den Ausgangspunkt bilden seine Erfahrungen als Nervenarzt und dabei vor allem die Beobachtung, daß in unserer Kultur Schuld- und Angstgefühle zu den stärksten dynamischen Faktoren bei psychischen Störungen gehören.«

1 http://schavanplag.wordpress.com/2012/06/16/seite-73/ (4.5.2013).

2 Heinz Häfner: Das Gewissen in tiefenpsychologischer Sicht. Einsiedeln 1967. S. 125.

Anstoß erregen hier nicht übereinstimmende Signifikanten (»Erfahrungen als Nervenarzt«, «stärksten dynamischen Faktoren« etc). Ohne gemeinsame Sprachausdrücke können wir nicht kommunizieren. Das Problem ergibt sich daraus, dass den Worten ein *Sinn* unterlegt wird, der erstens seine eigenen, erläuterungsbedürftigen, Identitätskriterien besitzt und, zweitens, regulativen Zuschreibungsbedingungen unterliegt, wie sie auch für wörtliche Zitate gelten.

Im Beispiel dreht es sich um das Verhältnis von Formulierungen wie »… auf der Basis therapeutischer Erfahrungen als Nervenarzt …« (Häfner) und »Den Ausgangspunkt bilden seine Erfahrungen als Nervenarzt.« (Schavan) Die Formulierung ist verschieden, die Sache ist dieselbe. Der Vorwurf lautet, dass die Paraphrase nur dazu dient, die Übernahme einer fremden Gedankenfigur zu verschleiern, die nicht mit einer konkreten Ausprägung zusammenfällt. An diesem Konflikt ist ein Kernpunkt des in sprachlicher Verständigung auftretenden Identitätsproblems sichtbar. Die Sache liegt nicht in der blanken Greifbarkeit einer Zeichenmanifestation. Verschiedene Grapheme können dasselbe bezeichnen. Die Bedingungen, unter denen die Urkundenforschung beurteilt, ob ein Dokument eventuell gefälscht ist, unterscheiden sich von einer hermeneutischen Untersuchung, ob zwei Autorinnen mit unterschiedlichen Worten dieselbe Mitteilung gemacht haben. Die Formulierungskünste Annette Schavans zeigen, dass identifizierende Zuschreibungen eine Reihe verschachtelter Praktiken voraussetzen. Es ist nicht so, dass Identität herrscht und sich da-

raus Differenzierungen ergeben, sondern andersherum. Wir beherrschen differenzierte Reaktionsweisen, aus denen sich Identifikationen herauskristallisieren.

Man könnte einwenden, diese sprachphilosophischen Anmerkungen hätten nichts mit Körpern zu tun, auf welche es in der Biometrie ankommt. Körper sind keine ätherischen Konstrukte wie Bedeutungen, sondern gehören auf die Seite physisch realisierter Zeichen. Die Probleme, welche sich in diesem Zusammenhang ergeben können, gleichen jenen der Urkundenforschung: Ist dieser Organismus genau jener, der in einem anderen Kontext markiert worden ist? Identifikation ist in diesem Zusammenhang die Feststellung der Übereinstimmung zweier zeitlich konstanter, sinnlich zugänglicher materieller Ensembles. Die logische Notation »a = a« gibt die Rahmenbedingung wieder, nach welcher »ein Etwas« einem anderen Etwas gleichzusetzen ist. Dazu kommt die Greifbarkeit einer solchen Gegebenheit. Der Koffer in der Gepäckauslieferung ist derselbe, der eingecheckt wurde; die Frau, die meinen Antrag bearbeitet, ist jene, die im Auto vorbeifährt. Doch diese handfeste Betrachtungsweise führt, was Identität betrifft, auf keinen sichereren Boden, als den vorhin angegebenen. Der Grund liegt darin, dass wir dieses Prädikat nicht nur in jenen Fällen verwenden, in denen wir uns mit einem doppelt gesetzten Namen zweimal auf dasselbe Ding beziehen. Wir können ein Ding auch so identifizieren, dass wir zwei verschiedene Bezeichnungen verwenden. »XY135 ist mein Koffer«. Damit sind wir im Bereich unsinnlicher Bedeutungen.

Zur Wirksamkeit identifizierender Aussagen gehört die Möglichkeit, ein Objekt als Bezugspunkt unterschiedlicher Gegebenheitsweisen festzuhalten. G. Frege hat das den Sinn sprachlicher Ausdrücke genannt. Sein berühmtes Beispiel ist die Bezugnahme auf den Planeten Venus durch die Terme »Morgenstern« und »Abendstern«.[3] »Der Morgenstern ist der Morgenstern« folgt dem Muster »a = a« und ist empirisch uninformativ. Dagegen enthält »Der Morgenstern ist der Abendstern« (a = b) eine verifizierbare Behauptung. Den darin angesprochenen Sachverhalt muss man entdecken, d.h. unter bestimmten Bedingungen, nach gewissen Kriterien, festschreiben. Vorstellbar wäre ja z.B., dass eine Sprachgemeinschaft den Zeitpunkt der Sichtbarkeit eines Himmelskörpers für so entscheidend hält, dass die materielle Gleichheit in den Hintergrund tritt. Man kann verstehen, wenn jemand sagt »Es *ist nicht* derselbe Pokal, wenn er nach einem sportlichen Erfolg verliehen oder am Flohmarkt erworben wird.« Die vielfältigen Sinnzusammenhänge, in denen sich materielle Gegebenheiten darstellen, unterscheiden sich nicht im Prinzip von den Bedeutungsschattierungen, die wir anhand der Plagiatsvorwürfe diskutiert haben. Informative Identitäten beruhen auf einer Doppelperspektive, welche unterscheidbare Hinsichten als Bezugnahme auf einen ununterschiedenen Referenzpunkt darstellt.

3 Gottlob Frege: Funktion, Begriff, Bedeutung. Fünf logische Studien. Herausgegeben und eingeleitet von Günther Patzig. Vandenhoeck & Ruprecht, Göttingen 1962. S. 38–63.

Der Identitätsbegriff ist nicht so einfach gebaut, wie es zunächst den Anschein hat. Dass etwas »mit sich selbst identisch ist« gilt als inhaltslose Tautologie, doch die Nachfragen können schon an diesem Punkt einsetzen. Zweimal mittels derselben Termini auf etwas zu referieren impliziert bereits eine Differenz in Zeit und Zeichengebrauch. Die Aussage, etwas ruhe in sich selbst, bedient sich einer Verdoppelung, die im nächsten Schritt zurückgenommen wird. Identität ergibt sich vor dem Hintergrund der Möglichkeit des Auseinanderfallens der beiden aufeinander bezogenen Komponenten. Sie ist eine Relation, die einem Ding zugeschrieben wird, sofern es *nicht* auf anderes bezogen ist. Insofern ist verständlich, dass Derrida die Herkunft der Identität in der Differenz reklamiert. Die originär wiederholende Struktur[4] des Zeichens beruht darauf, dass es kein *einmaliges* Zeichen gibt. Damit etwas als Zeichen verstanden werden kann, muss es in eine differentielle Struktur eingebunden sein. Nur aufgrund der *Wieder*erkennbarkeit (von Sprachausdrücken und von Gegebenheiten) statuieren wir ihre Konstanz. Soweit die Hinweise auf die Praxis der Identifikation. Als zweiter Themenkreis sind Messverfahren zu betrachten.

messen

Ein Ding, oder ein Prozess, kann als Informationsträger betrachtet werden. Bäume haben eine bestimmte Höhe, Kochvorgänge beanspruchen bestimmte Zeit. Der Umgang mit solchen Daten lässt sich in Variablen operatio-

4 Jacques Derrida: Die Stimme und das Phänomen. Frankfurt/Main 2003. S. 69f.

nalisieren, also z.B. in Vorkehrungen zur Höhenmessung. Der Messvorgang richtet sich auf geeignet festgelegte, quantifizierbare Eigenschaften (Variablen) von Dingen bzw. Prozessen und übersetzt sie, zumeist mit Hilfe technischer Geräte, in skalierte Werte. In Einführungen zur Messtheorie ist die Rede von »wahren Variablen«, die als Input und »gemessenen Variablen«, die als Ergebnis des Messvorgangs bezeichnet werden.[5] Im Idealfall würden die beiden Größen zusammenfallen, normalerweise sei allerdings mit der Eigengesetzlichkeit der Messsysteme zu rechnen. Gegenüber den als unvermittelt gedachten Originalzuständen sind Messresultate von den Vorkehrungen zur Erfassung der Variablen abhängig. Der Begriff einer »wahren Variablen« wird dadurch in doppelter Weise verkompliziert.

Einerseits stellt sich die Frage, ob eine Messung als Kombination eines für sich bestehenden Wertes und eines Fehleranteils verstanden werden soll. Wenn eine Ungenauigkeit des Messgeräts bekannt ist, kann sie aus dem Ergebnis herausgerechnet werden. Die Uhr, welche zu langsam geht, ist auf diese Weise auch noch nach einer Woche verlässlich. Doch das Konzept der Ungenauigkeit hängt seinerseits von einer sachadäquaten Ausgangslage ab und diese Information ist nur durch eine Messung zugänglich, in welcher ihrerseits mit einem Fehleranteil zu rechnen ist. Der »wahre« Wert der Variable wird also nicht gemessen, sondern als Grenzfall aus fehleranfälligen Messungen zurückextrapoliert. In

5 Vgl. etwa John B. Bentley: Principles of Measurement Systems. Harlow 2005. S. 3.

dieser Hinsicht ist er einer der Faktoren in der Kalibrierung entsprechender Systeme, keine unabhängige, einfach zu registrierende, Gegebenheit. Sorgfältig kalkulierte Szenarien gewährleisten die erwünschten, praktisch verwendbaren, Funktionszusammenhänge. Eine zweite Überlegung nimmt aus weiterreichenden Gründen Anstoß an »wahren Variablen«. Diese Redensweise erweckt nämlich den Anschein, als hätte man, gegeben ein definitiv gültiges Messverfahren, auch ohne Messverfahren Zugang zu den – noch dazu gültigen – Informationen. Die erwünschte Praktikabilität wäre mit einer unerschütterlichen Legitimität verbunden.

Das Bedenken hat Emanuel Derman, ein Physiker und Finanzmathematiker, konzis auf den Punkt gebracht: »Es gibt keine ‚Rohdaten'. Die Entscheidung, welche Daten man sammelt, bedarf bereits der Einsicht.«[6] Die Schwierigkeit besteht nicht darin, möglicherweise auftretende Messfehler auszuschließen, um an die objektiven Gegebenheiten zu kommen. Sie liegt in der Unterstellung, Informationen wären ohne den aktiven Eingriff einer Fragestellung gegeben und könnten, wenn man von deren Anteil abstrahiert, als »unverdächtige« Bestätigung reklamiert werden. Die Messmethode erschließt das Feld, welches sie auf inventarisierbare Sondierungsergebnisse abcheckt. Um den Einfluss von Willkür zu vermeiden wird das methodologisch kontrolliert. Es ist möglich, für gegebene Zwecke eine Bandbreite akzeptabler Variablen-

6 Frankfurter Allgemeine Zeitung, 6.3.2013. http://www.faz.net/aktuell/feuilleton/modelle-die-sich-schlecht-benehmen/kolumne-von-emanuel-derman-wenn-daten-den-verstand-verhexen-12103683.html (15.4.2013).

werte anzugeben. Doch es ist sinnlos, nach einem Wert zu suchen, der vor dieser Intervention besteht. Prägnanter: »Daten haben keine Stimme«[7]. Die Umstände, unter denen wir leben, sprechen nicht zu uns. Sie machen sich, so kann man es vielleicht formulieren, bemerkbar, doch diese Interferenz mit menschlichem Verhalten ist nur distinkt, wenn sie sprachlich, und damit sozio-kulturell, aufgenommen wird.

Aus philosophischer Sicht überraschen diese Zusammenhänge nicht. In einer berühmten Passage charakterisiert Immanuel Kant das wissenschaftliche Verfahren so, dass die Naturforscher »begriffen, daß die Vernunft nur das einsieht, was sie selbst nach ihrem Entwurfe hervorbringt.«[8] Theorie und Experiment richten sich auf die Natur, »aber nicht in der Qualität eines Schülers, der sich alles vorsagen läßt, was der Lehrer will, sondern eines bestallten Richters, der die Zeugen nötigt, auf die Fragen zu antworten, die er ihnen vorlegt.«[9] Hegel hat die Kantische Pointe radikalisiert, indem er darauf hinwies, dass nicht nur empirische Untersuchungen, sondern auch deren methodologische Reflexion als voreingenommen zu betrachten seien. Kants vorgeblich neutrale Untersuchung des menschlichen Erkenntnisvermögens setzt, so lautet Hegels Einwand, manches »als Wahrheit voraus und stützt darauf ihre Bedenklichkeiten und Konsequen-

7 a.a.O.

8 I. Kant, Kritik der reinen Vernunft, Vorrede zur zweiten Auflage, B XIII.

9 a.a.O.

zen, was selbst vorher zu prüfen ist, ob es Wahrheit sei.«[10] Nur der gesamte Prozess, in welchem die Annäherung an den Erkenntnisgegenstand diesen zunächst als an sich gelten lässt und dann als eine für sie selbst gegebene Position begreift, wird der Komplexität der Erkenntnisbewegung gerecht.

Für Messverfahren und Maßstäbe gilt also, wie für Identität, dass sie einer detaillierten Analyse bedürfen. Die Ermittlung »gemessener Variablen« ist nur eine vorläufige Beschreibung. Mit dem Begriff der Messung sind Nachfragen nach der gewählten Messmethode und den in sie investierten Interessen unweigerlich verbunden. Die Aufgabe, die sich aus dieser Konstellation ergibt, besteht darin, der Versuchung zweier Extrempositionen zu entgehen. Die eine sagt in etwa: »Intelligenz ist, was der Intelligenztest misst«, die andere: »Wir messen, worin Intelligenz besteht«. Allgemeiner ausgedrückt: die »wahre Variable« wird mit der gemessenen konfundiert oder als Datum außerhalb des Tests vorausgesetzt. Eine Zwischenposition muss damit umgehen, dass weder der Maßstab noch das Gemessene als unabänderlich betrachtet werden können. Hegel hat es nachhaltig formuliert: »… der Maßstab der Prüfung ändert sich, wenn dasjenige, dessen Maßstab er sein sollte, in der Prüfung nicht besteht …«[11] Der Philosoph entwickelt daraus eine Dialektik. Moderner kann man von Rückkoppelung sprechen. In der Praxis unterliegen unsere Vermessungen einem

10 G.W.F. Hegel, Phänomenologie des Geistes. Werke 3, Frankfurt/Main 1970. Einleitung S. 69f.

11 a.a.O. S. 76.

vorweg nur begrenzt bestimmbaren Unsicherheitsfaktor. Das liegt nicht an mangelnder Präzision, sondern an der Tätigkeit selber, die wir betrachten.

Identität messen

»Identitätskontrolle« klingt so, als ließe sich Identität wie Geschwindigkeit oder Zugangsberechtigungen kontrollieren. De facto wird der Terminus ja auch auf diese Art gebraucht. Ausweispapiere oder, das war das Thema des Berliner Workshops, biometrische Daten, fungieren als Maßstab, um »die Identität festzustellen«. Die beiden vorangegangenen Abschnitte haben gezeigt, dass sowohl die Rede von Identität, als auch jene von Messvorgängen, bei näherem Zusehen komplexe Sachverhalte bezeichnet. Entsprechend mehrschichtig ist die Formulierung »Identität messen«. Im einfachsten Fall besagt sie, dass in bestimmten Bezugssystemen Gegebenheiten fixiert und durch quantitative Überprüfung (wiederholt) referenzierbar gemacht werden. So wird nachgemessen, ob ein Bremsbelag ausgetauscht oder ein Medikament verfälscht worden ist. Auch DNA-Spuren gehören in diese Rubrik. Und schließlich: Mittels genetischer Tests lässt sich feststellen, dass biologische Substanzen vom selben Lebewesen stammen.

Dass es bei einfachen Fällen nicht bleibt, ergibt sich aus der Sinnabhängigkeit der praktisch verbreiteten Identitätsaussagen. Der genetische Fingerabdruck A ist gleich eben demselben Abdruck A, aber interessant ist doch, ob ein Abdruck B, der aus anderen Umständen stammt, dem Abdruck A gleicht. Mit empirisch erhobenen Iden-

titäten verhält es sich darum nicht anders als mit den Vergleichsstellen eines präsumtiven Plagiats. Das Urteil über die Gleichheit kann sich nicht nur am Augenschein orientieren, sondern muss Rahmenbedingungen mit berücksichtigen. Unterschiedliche Hinsichten auf eine Sache sind eben doppelt verfasst: divergent hinsichtlich der Kontexte und konvergent hinsichtlich eines Bezugspunktes, der aus den Kontexten extrahiert wird. Ein aufgefundener Fingerabdruck kann einem vorliegenden Exemplar gleichen, aber damit ist noch nicht gesagt, wie diese Abstraktion zu beurteilen ist. Aus Kriminalfilmen sind mehrere Strategien bekannt, die aus der Abstraktion erschlossenen Identitäten zu unterwandern. Biometrie ist demnach, wie andere Strategien der Identitätsfeststellung, in zweifacher Perspektive zu sehen. Sie bietet die operative Möglichkeit eines Kennzeichnungs- und Wiedererkennungsregimes, sie unterliegt aber gleichzeitig den Interessensvorgaben, welche – zu jeweiligen Zwecken – Invarianten aus den immer auch konfusen Weltabläufen herausheben.

Eine Kombination von handfesten Bestandsaufnahmen und Überraschungen, die niemals auszuschließen sind, kennzeichnet die Biometrie. An dieser Mischung entzünden sich praktisch-politische Probleme, doch das ist hier nicht das Thema. Zur Analyse der methodischen Zusammenhänge im Rahmen der Wiedererkennung eignet sich, abschließend, eine Notiz aus Ludwig Wittgensteins Nachlass. Sie steht im Zusammenhang mit Überlegungen zu Begriffen als Stationen im Lebenszusammenhang. »Der Hintergrund ist das Getriebe des Lebens. Und un-

ser Begriff bezeichnet etwas in diesem Getriebe.«[12] Er soll sich auf dieselbe Sache beziehen, andernfalls ist er äquivok. Doch diese Identitätsbedingung schließt Unsicherheit nicht aus. Sofern Begriffe auf Weltzustände zugreifen, hängen sie auch von ihnen ab. Wittgenstein diskutiert die Konstellation anhand eines Beispiels, das aus einem Avantgardefilm genommen sein könnte. Gegeben sei ein Streifen, der ein regelmäßiges Bandmuster enthält. Auf diesem Streifen, und damit auch auf diesem Muster, wird eine Malerei aufgetragen und mit Hilfe des Musters beschrieben.

»Wenn das Muster liefe: a b c a b c a b c … , so hätte ich einen besonderen Begriff dafür, dass etwas Rotes auf ein c fällt und etwas Grünes auf das nächste b.«[13] Jemand fährt eine Allee entlang und klebt auf jeden dritten Baum ein Plakat, auf jeden zweiten einen Lampion. In derartigen Vorgängen sind drei Komponenten von Bedeutung. Zunächst der Ablauf (1) eines Musters (2), d.h. eine Regelmäßigkeit in der Zeit, die quasi einen Rhythmus vorgibt. Vor diesem Hintergrund wird eine individuelle Gestalt (3) aufgetragen. Sie steht nicht isoliert im Raum, sondern bezieht ihre Koordinaten von einem ablaufenden Band. In dieser doppelten Zeitabfolge liegt die Pointe. Die Szene besteht *nicht* aus wechselnden Ereignissen in einer gleichbleibenden Umgebung, sondern die verschiedenen Malereien sind ihrerseits an einen – vorhersehbaren – Ablauf gekoppelt. Bei der Identifikation eines Ereignisses

12 Wittgenstein's Nachlass. The Bergen Electronic Edition (BEE, Oxford University Press 2000). Manuskript 137, S. 29a.

13 a.a.O. S. 99a.

spielt der »Rhythmus« im Hintergrund eine unerlässliche Rolle. Ein Pinselstrich, um im Bild zu bleiben, kommt in diesem Szenario nicht einfach vor, sondern hängt funktional mit einem vorgegebenen Muster zusammen. Die Definitheit eines Begriffes zeigt sich in seiner Applikation auf wiederkehrende Umstände.

Die Bedeutung dieses Bildes für Identitätsmessungen liegt darin, dass es plastisch zeigt, wie sich Konstanz und Variabilität in Anwendungsfällen zu einer semi-stabilen Kombination zusammenschließen können. Testergebnisse basieren, wie Begriffe, auf vorausgesetzten Regularitäten. Das ist Wittgensteins wiederkehrendes Muster. Die Überwachung der Betriebstemperatur einer Industrieanlage erfordert festgeschriebene Prozeduren, die für eine bestimmte Bandbreite gültige Messergebnisse liefern. Wenn im Prozessstadium c ein grünes Signal auftritt, erfüllt die Installation ihren Zweck. Unter solchen Voraussetzungen ist man geneigt, davon zu sprechen, dass ein Instrument eine Maschine erfolgreich kontrolliert, oder, auf das Tagungsthema bezogen, dass biometrische Verfahren ihren Zweck erfüllen. Doch wir sprechen über einen Ablauf in der Zeit. Die Regelmäßigkeit des Musters, die aus punktuellen Interventionen sinnvoll platzierte Zeichen macht, ist letztlich nicht verbürgt. »Wenn nun einmal Anomalien in dem Muster auftreten, so werde ich im Zweifel darüber sein, welches Urteil zu fällen ist.«[14] Der Hintergrund selbst kann sich verschieben. Das Prozessstadium c ist gestört. Was bedeutet dann ein grünes Signal?

14 a.a.O.

Die korrekte Antwort kann nur sein: »Das kommt darauf an.« Ein Wechsel oder Ausfall der Bedingungen, zu welchen das Zeichen passt, erzeugt Unsicherheit. Anders gesagt: als Zeichen kann es fungieren, wenn es semiotisch nachvollziehbar mit anderen Ereignissen verbunden ist. Ihr Ausbleiben kann, streng genommen, nicht zur Folge haben, dass ein Zeichen ohne Referent übrig bleibt. Stattdessen haben wir es mit einer Zeichengestalt zu tun, deren Zweck und Bedeutung in Schwebe bleibt. Ein Grünsignal bei defekter Maschine kann heißen, dass dieses Zeichen nicht mehr für Funktionstüchtigkeit steht; oder dass es bereits zuvor nicht für sie (sondern für einen anderen Parameter) stand; oder dass das Gerät gar nicht defekt ist. Ohne eine ceteris paribus Stabilität gibt es keine Identifikationen, aber es gilt auch, dass dieser Faktor seinerseits nicht auf dieselbe Weise wie der Identifikationsprozess kontrollierbar ist.

Um feststellen zu können, ob zwei Gegebenheiten gleich sind, müssen Umstände gleich bleiben. Umstände aber sind andersartig gleich als Gegebenheiten.

»How to liquefy a moving body: Eurodac und die Digitalisierung der Europäischen Grenze«

Brigitta Kuster & Vassilis S. Tsianos

Wir werden heute ausschnitthaft aus unserer Forschung im Rahmen des im 7. Europäischen Rahmenforschungsprogramm angesiedelten Projektes Mig@Net berichten. Unser Beitrag heute beschäftigt sich am Beispiel von Eurodac mit der Digitalisierung der europäischen Grenzkontrolle. Eurodac ist eine Informations-, Kommunikations- und Kontrolltechnologie. Es ist der Name einer europäischen Datenbank, in der die Fingerabdrücke von Asylsuchenden und irregulären MigrantInnen in einem so genannten Automatischen Fingerabdruck-Identifikations-System (AFIS) gespeichert werden. Den politischen Geltungsraum dieses Systems bildet die Dublin-II-Verordnung, die als Antwort auf die Krise des europäischen Asylsystems konzipiert worden ist – begleitet von der Konstruktion und dem Gebrauch von so flapsigen Begriffen wie „refugees in orbit" und „asylum shopping".[1]

1 Wie Dublin II ist auch Eurodac eine Regulation, die vom Europäischen Rat am 11. Dezember 2000 als Dublin-bezogene Maßnahme erlassen wurde. Für eine Regulation im Bereich der Asylpolitik bedurfte es damals, d.h. vor dem Inkrafttreten des Vertrags von Lissabon 2009, keiner parlamentarischen Zustimmung, sondern sie konnte direkt von der Europäischen Kommission veranlasst werden. Die Eurodac-Regulation lieferte die legale Grundlage für die Einrichtung eines europäischen digitalen daktyloskopischen Systems, welches biometrische Identifikationstechnologie und Informationstechnologie miteinander verbindet (Council Regulation (EC) 2725/2000).

Dublin II folgt dem Verursacherprinzip, welches besagt, dass der Mitgliedstaat, der die Einreise eines_r Asylantragssteller_in „verursacht" hat (etwa durch Vergabe eines Visums oder aufgrund mangelnder Sicherung der Grenze), das Asylverfahren durchführen muss. Indem es mit Hilfe der Datenbank Eurodac die Zuständigkeit eines und nur eines Mitgliedstaates pro Asylantrag rekonstruiert, bildet Dublin II das innere Regulativ der Mobilität von Nicht-EU-Staatsbürger_innen ohne Visum innerhalb der EU.

In der Regel werden Kontrolltechnologien zur Grenzsicherung entweder in ihren politischen Wirkungen erfasst und kritisiert – d.h. abgekoppelt von den technischen Infrastrukturen, die sie erfordern – oder aber technodeterministisch, im Sinne einer Axiomatik technischer Machbarkeit. Eine digital stabilisierte Grenze gilt somit meist als potenziell funktionstüchtig. Im Kontrast dazu verstehen wir unsere Forschung als einen ethnografischen Beitrag zum Verständnis der soziotechnologischen Emergenz der digitalen Grenze bzw. der Digitalisierung von Grenzkonflikten.[2] Unser Untersuchungsgegenstand lässt

Die Eurodac-II-Regulation vom Februar 2002 stellt den legalen Rahmen für die technische Operationalisierung des Systems bereit. Sie umfasst Regeln für den administrativen Unterhalt und die administrative Umsetzung wie etwa die Altersbeschränkung der daktyloskopisch zu Identifizierenden (Council Regulation (EC) No 407/2002). Inzwischen sind diese beiden Verordnungen durch Regulation (EU) No 603/2013 abgelöst worden.

2 Dieser Beitrag basiert auf der Feldforschung der Bordercrossing-Forschungsgruppe des Forschungsprojektes Mig@Net (Transnational Digital Networks, Migration and Gender, http://www.mignetproject.eu/), das im Rahmen des Siebten Rahmenforschungs-

zugleich Gesellschaft und Technik bzw. Migration und digitale Grenzkontrolle entstehen. Wir meinen allerdings, dass die Literatur zur Digitalisierung der Grenze häufig einer Art Blackbox-Epistemologie folgt, die das Objekt der Forschung, d.h., inwiefern Eurodac für das „doing border" einen Unterschied macht, in der Opazität belässt. Diese Geschlossenheit in einer Sequenz von Untersuchungen zu öffnen, eine Art De-Blackboxing-Operation durchzuführen, ist, so meinen wir, die Voraussetzung dafür, die digitale Grenze überhaupt erst in den Blick zu bekommen.

Ironischerweise ist der technologische Anteil des Objektes der Forschung, d.h. die in Luxembourg gelegene Eurodac-Central Unit, technisch gesehen eine buchstäbliche Blackbox: Wir kennen die Inputs und die Outputs und nur in diese lässt sich beobachtend oder manipulierend eingreifen; der zentrale Server ist ein vollautomatisches Lights-out-System, bei welchem sogar das Löschen von Daten selbsttätig erfolgt. Ein Interview, das wir 2011 mit der IT-Managerin Gilian Ormiston geführt haben, machte uns eine weitere Facette der Blackbox-Epistemologie deutlich. Als Frau in leitender Position eher eine Ausnahme im Bereich des IT-Managements beschrieb sie, wie

programms der Europäischen Union (FP7) angesiedelt ist. Ausführlicher Forschungsbericht siehe: http://www.mignetproject.eu/?cat=5. Die Forschungsergebnisse, die wir in diesem Beitrag diskutieren, stammen aus der Forschung von Dr. Vassilis Tsianos und Ph.D. candidate Brigitta Kuster, Universität Hamburg; Dr. Nelli Kambouri, Ph.D. candidate Olga Lafazani und Dr. Dimitris Parsanoglou, Centre for Gender Studies, Panteion University, Athen; Dr. Renata Pepicelli, Universität von Bologna.

sie 2003 den logistischen und technischen Aufbau von Eurodac geleitet hat: „It is not about IT, it is about people. People are making IT." Sie stellte heraus, dass der Aufbau von Eurodac nicht nur Projekte des Datenaustauschs mit damals 16 Mitgliedsstaaten umfasste, sondern parallel dazu auch der Herstellung eines Kommunikationsnetzes bedurfte. „Communication is something else then data exchange." Frau Ormiston brachte uns bei, endgültig mit der Vorstellung zu brechen, dass Kontrolltechnologien, in unserem Fall biometrische Identifikationstechnologien, primär technologisch sind.

Numbers that Matter

Der Moment, in dem wir im Herbst 2010 die Ausgangspunkte unserer Forschung formulierten, fiel zeitlich mit der Ausrufung des Schengener Ausnahmezustandes und in der Folge dem ersten RABIT-Einsatz von Frontex an der griechisch-türkischen Evros-Grenze zusammen.[3] Als erfahrene GrenzregimeforscherInnen mit dem Ziel, die Grenze in situ und in actu zu ethnografieren, folgten wir dem Reflex, möglichst zeitnah das Feld des Kriseneinsatzes, der den topologischen Grenzraum betraf, zu erkunden. Als ForscherInnen jedoch, die sich ins Feld der digitalen Grenze vorwagten, beschlichen uns einige Zweifel

3 RABIT ist das Akronym für „Rapid Border Intervention Teams" (siehe dazu auch: Verordnung (EG) Nr. 863/2007 des Europäischen Parlaments und des Rates vom 11. Juli 2007 über einen Mechanismus zur Bildung von Soforteinsatzteams für Grenzsicherungszwecke und zur Änderung der Verordnung (EG) Nr. 2007/2004 des Rates hinsichtlich dieses Mechanismus und der Regelung der Aufgaben und Befugnisse von abgestellten Beamten).

darüber, ob eine solche Feldforschung auch fähig wäre, die digitale Dimension der offensichtlichen Krisenaktualität dort in der Evros-Region zu lokalisieren. Mit anderen Worten, wir stellten uns in Anlehnung an Rabinows Überlegung der „anthropology of the actual" (2003) die Frage, was die digitale Aktualität dieser Grenze wäre und welcher Praxen es bedarf, sie zu beforschen. Bei der Beschäftigung mit Eurodac fiel uns auf, dass die 2011 in den europäischen politischen Institutionen proklamierte Krise bereits in den Zahlen und ihrer Interpretation ablesbar war, die der Eurodac-Tätigkeitsbericht von 2010 für das Jahr 2009 konstatierte. Darin ist von einem markanten Abfall der Datenkurve derjenigen Personen, die illegal die EU-Außengrenze überschritten haben, die Rede: „Beim Trend der illegal über eine Außengrenze eingereisten Personen (‚Kategorie 2') waren 2009 gravierende Änderungen festzustellen. Nach einem Anstieg um 62,3% zwischen den Jahren 2007 und 2008 (auf 61.945) fiel die Anzahl der Dateneingaben 2009 um 50 % (auf 31.071): Die meisten dieser Daten werden von Italien, Griechenland und Spanien eingegeben. Davon gibt Griechenland die meisten Daten ein – 2009 übermittelte dieser Mitgliedstaat 60 % aller ‚Kategorie 2'-Daten (18.714 verglichen mit 20 012 im Jahr 2008)." (KOM 2010 415 endgültig, S. 5)

Dieser Brüsseler Bericht handelt nicht von einem Geschehen im soziologischen Sinne, sondern er zählt, kombiniert und ordnet Zahlen, genauer: digitale Aufnahmen von Fingern, die an unterschiedlichsten Orten im Schengener Grenzraum gemacht worden sind, gemäß bestimmter zeitlicher und räumlicher Kategorien. Er-

hoben werden die Zahlen entlang des Geschlechts und Alters der FingerträgerIn, des Ortes ihres Aufenthalts zum Zeitpunkt der Registrierung ihrer Finger und einer möglicherweise folgenreichen Eurodac-Kategorisierung: Kategorie 1 steht für AsylbewerberInnen, Kategorie 2 für AusländerInnen, die illegal die EU-Außengrenze überschritten haben, und Kategorie 3 für illegale MigrantInnen innerhalb von Schengen.[4] Diese kategorisierende Zählung zielt – wie Irma van der Ploeg prägnant gezeigt hat – weniger auf eine bessere Kenntnis von Drittstaatenangehörigen, sondern auf eine „Informatisierung des Körpers" (Ploeg 2005), der die Flüchtigkeit der grenzüberschreitenden migrantischen Körper lesbar machen soll (Ploeg/Sprenkels 2011). So etablieren die Eurodac-Zahlen und -Kategorien eine „verkörperte Identität der Migration" (Tsianos/Kuster 2012) im Schengener Raum,[5] die sich verifizieren lässt und die alljährlich von einem öffentli-

4 Siehe Council Regulation (EC) 2725/2000.

5 In der Sprache der Programmierung entspricht die „Identifikation" einer Eins-zu-Viele-Suche innerhalb einer gegebenen Datenbank mittels Mustererkennungsalgorithmen. Im Gegensatz dazu entspricht eine „Verifikation" einem Eins-zu-Eins-Treffer. Diese Unterscheidung widerspiegelt die Differenz zwischen Wahrheit und Identität, wie sie im westlichen (Alltags-)Denken etabliert ist. Während die Wahrheit zu erlangen dem Versuch entspricht, die Vermittlung zu liquidieren und auf diese Weise Deckungsgleichheit zu erreichen, ist Identität immer schon konfrontiert mit den Schwierigkeiten des Prozesses, Vielheit abzuziehen. Authentizität wiederum versucht, die Subtraktion der Vielheit der Identität im Singulären anzutreffen. In der Sprache der biometrischen Matcher haben verification und authentication die gleiche Bedeutung. (Siehe auch: The Biometrics Blog online: http://www.360biometrics.com/blog/difference-between-identification-authentication/)

chen Bericht reflektiert wird. Anders, als wenn ein Forscher vom Hügel auf den Grenzfluss hinunter schaut und die dortigen Bewegungen von Grenzpolizei, Frontex und TransitmigrantInnen beobachtend zu verstehen sucht, wie wir das auch taten, rekombiniert und interpretiert die SchreiberIn (und die LeserIn) des Eurodac-Berichts Zahlen. Aufgrund des Algorithmus', dessen Funktion darin besteht, die Verbindungen zwischen Punkten zu errechnen, entfaltet der Eurodac-Bericht ein numerisches Geschehen. Von den registrierten Nummern gehen Vorgänge aus, die sich mit Bruno Latours Begriff der Inskription fassen lassen und als die Aktivität „unveränderlich mobiler Elemente" (Latour 2006) verstanden werden können. Bereits für das Jahr 2009 protokollierte die Inskription eine (statistisch unterstrichene) Auffälligkeit an der griechischen Schengener Grenze, deren Aktivität 2011 aus dem Protokoll heraustrat. Die Zahlen haben sich offenbar 2011 – und das ist das Entscheidende – an die griechische Schengener Grenze verlagert, wo sie infolge eines Statuswechsels ein neues Leben als Bedeutungs- und Legitimationsträger für die laufende RABIT-Intervention zu führen begannen. Wir verstehen die Eurodac-Zahlen somit als mobile, unveränderliche, präsentierbare, lesbare und miteinander kombinierbare Inskriptionen, die als Referenten einer mobilen migrantischen Identität zirkulieren und diesbezügliche Mobilisierungsprozesse zu beschleunigen und zu bündeln im Stande sind. Wie das geschieht, versuchen wir im Folgenden zu rekonstruieren,

indem wir einige Aktivitäten und Orte des Eurodac-Akteur-Netzwerkes in den Blick nehmen und dabei neue Verbindungen ziehen.

Die Produktion von Inputs und Outputs

In unserer Absicht, solche Lokalisierungen vorzunehmen, durch die sich die technische, politische und institutionelle Arbeit an den Erfolgen beobachten lässt, die an der Grenze mit den In- und Output-Zahlen von Eurodac erzielt werden, stießen wir selbstverständlich auf die deutsche Eurodac-Zentralstelle im Bundeskriminalamt in Wiesbaden, wo das große deutsche elektronische Fingerabdruckarchiv residiert.[6] Im Laufe unseres Interviews mit dem Chef des deutschen AFIS (welches mehr als 3,5 Millionen Datensätze umfasst) im Juni 2011, fragte uns dieser aufrichtige homo faber, ob wir als FeldforscherInnen an der südeuropäischen Grenze das Motiv seiner griechischen KollegInnen kennen würden, eine so große Anzahl von Einträgen in Eurodac unter der Kategorie 2 der „illegal border crossers" zu produzieren. Er kommentierte diese Zählweise als eine Praxis, die seiner Meinung nach weder aus technischer noch aus logischer Sachvernunft nachvollziehbar und vertretbar sei, sondern das Ergebnis eines politischen Kompromisses darstelle. Über die griechische Zahl machte er die folgende Bemerkung: „In Italien ist die Zahl dieser Einträge inzwischen in der Tat zurückgegangen. Es scheint ein Sinneswandel stattgefunden zu haben… Warum benutzt Griechenland die Kategorie 3 nicht? Ich verstehe das nicht. Gebt mir Be-

6 Siehe etwa auch Töpfer 2008.

scheid, wenn ihr etwas darüber herausfindet. Wenn sie die Kategorie 3 verwenden würden, könnten sie viele Asylbewerber loswerden." – Aus den Erwägungen dieses Kriminalbeamten wird ersichtlich, dass im BKA offenbar ein national und institutionell breiter und dezentraler Raum für unterschiedliche Strategien und Taktiken eingeräumt wird, wenn es um die quantitative und qualitative Datenzufuhr zur Eurodac Central Unit geht. Ganz im Sinne der multisited ethnography haben wir die Frage des deutschen Polizeioffiziers aufgegriffen und uns somit auf eine Spur gesetzt, die das Feld selbst erzeugt hat. Der Versuch, uns Einsicht zu verschaffen an jenen Knotenpunkten des Akteur-Netzwerks von Eurodac, die unserem Interviewpartner vom Bundeskriminalamt offenbar unzugänglich geblieben sind, führte uns zu einem Polizeioffizier in der zentralen nationalen Eurodac-Verbindungsstelle in Athen, der uns die Funktionsweise von Eurodac in einer anderen, aber nicht weniger eigenwilligen Weise erläuterte. Während er auf dem Bildschirm eine Hit-Meldung zeigte, erklärte er: „Zum Beispiel diese Person hier hat in Griechenland Asyl beantragt, seine [sic!] Fingerabdrücke wurden aber zuerst in Schweden registriert. Es scheint sich hier also um einen Fall zu handeln, für den Schweden zuständig ist. Die Person sollte nach Schweden geschickt werden. Natürlich könnte es sich hierbei um eine falsche Information handeln, denn: Wie könnte diese Person direkt nach Schweden gelangt sein? Aller Wahrscheinlichkeit nach ist sie zuerst nach Griechenland eingereist, dabei aber nicht registriert worden oder aber man hat sie bei der Einreise als Kategorie 2

registriert und dieser Eintrag ist dann gelöscht worden, so dass ihre Fingerabdrücke zum ersten Mal in Schweden auftauchen."

Über die Tatsache hinaus, dass dieser Polizeibeamte wie selbstverständlich einräumt, dass illegale Einreisen nach Europa via Griechenland nicht selten unregistriert stattfinden, sind an seiner Beschreibung zwei weitere Aspekte erstaunlich. Zum einen berichtet der Polizeibeamte implizit von einer Migrationsroute nach Europa, die mittlerweile offenbar ins Visier der Polizei geraten ist. Die Route, von der die Rede ist, ist allerdings weniger geographischer Art als dass sie durch Zeiträume gekennzeichnet ist, denn nach den Regeln der Eurodac-Regulation müssen die Fingerabdruckdaten unter Kategorie 2 (Kategorie illegaler Eintritt über die EU-Außengrenze) nach zwei Jahren gelöscht werden.[7] Diese Daten dürfen nicht zum Anlass genommen werden, eine Recherche in der Eurodac-Datenbank vorzunehmen, sie dienen lediglich als Vergleichsmaterial für die Suchaufträge, ausgehend von Kategorie-1-Einträgen. Diese Einschränkung ist Teil des politischen Kompromisses, auf den wir beim BKA hingewiesen wurden.[8] Zweitens lässt sich die Beschreibung des griechischen Beamten als Hinweis auf eine Pragmatik interpretieren, in der sich in Griechenland eine Antwort auf die Frage formiert, die der Beamte im Bundeskriminalamt Wiesbaden aufgeworfen hat. Im Selbstverständnis weiterhin, immer noch oder sogar immer mehr erneut Transitland, ist die Differenz in der

7 Siehe Council Regulation (EC) 2725/2000.

8 Siehe dazu detaillierter: Aus 2003, Aus 2006.

Illegalität, je nachdem ob sie sich auf die Grenze oder auf das Territorium bezieht, nicht so entscheidend. Die Spitzfindigkeit einer solchen Unterscheidung wird genauso nach Europa verwiesen, wie Europa auf Griechenland als europäische Grenze verweist. Derweil lässt sich dennoch genau das erzielen, was der BKA-Offizier als Interesse postulierte: Zahlen und Inskriptionen generieren, die dabei helfen, die Asylsuchenden loszuwerden.

„The glass is dangerous"

Es ist nicht nur von historischem Belang, dass Eurodac als Reaktion auf die Turbulenzen der Migration in Europa bzw. die Bewegungen von Migrant_innen innerhalb des Schengener Raumes entstanden ist. Folgt man der Literatur, so sind die Migrant_innen, welche Eurodac beziffert, dagegen komplett von der Funktionsweise dieses Informations- und Kontrollsystems abgekoppelt. Das dürfte der Grund sein, warum in der Eurodac-Forschung das Wissen der Migration implizit, als weitgehend irrelevant taxiert, kaum berücksichtigt wird. So entsteht das Bild eines manichäischen Verhältnisses zwischen Agenten und Wissensformen der Kontrolle und Agenten und Wissensformen der Mobilität, das – um mit Peter Shields (2010: 277) zu sprechen – Gefahr läuft, zu einer „eskalierenden Dialektik der Kontrolle" beizutragen, indem es an der Formung derjenigen Symptome mitwirkt, die es eigentlich aufzulösen beabsichtigt – z.B. der starke Fokus auf technische Lösungen, um die Grenze zu überwachen und zu kontrollieren. Akteur-Netzwerke, in denen Informationen über Migration und ihre Kontrolle zirku-

lieren mittels einer „n(e)thnografischen Grenzregimeforschung“ (Pieper/Kuster/Tsianos 2011) in der Perspektive der Migration zu beforschen, bedeutet dagegen, sich an die Fersen bzw. die Finger der Migration zu heften. Deshalb kommt in unserer Akteur-Netzwerk-Rekonstruktion von Eurodac den Erzählungen über die Fingerabdruckentnahme der TransitmigrantInnen auf ihrer Weiterreise innerhalb des Schengener Territoriums privilegierte Bedeutung zu. Auf diese Weise adressiert uns innerhalb der internen Komplexität einer digitalen Grenze die Emergenz des aktuellen Konflikts um die Grenze in der Perspektive der Migration. Migration kommt zuerst. Bewegung kommt vor ihrer Kontrolle.

Im Frühjahr 2011 waren wir zum ersten Mal in Igoumenitsa. Es ist das letzte griechische Hafenstädtchen zu Italien vor der Grenze zu Albanien. Während unseres Aufenthaltes dort besuchten wir die informelle Siedlung der fast durchwegs männlichen Transitmigranten, die mittlerweile von der Polizei geschleift worden ist.[9] Sie war am Rande der Stadt, am Abhang direkt über der Zugangsstraße zum Hafen gelegen und wurde von den Bewohnern „the mountain“ genannt. Hier kam Rastaman auf uns zu, fragte uns nach einer Zigarette und erzählte von seiner Reise. Vom Sudan über Syrien, den Libanon, die Türkei und schließlich im November 2009 über die griechische Insel Lesvos sei er hierher gelangt. In Mytilini sei er nach wenigen Tagen festgenommen und

9 Siehe z.B. den Bericht zur Situation in Igoumenitsa von Ende Mai 2011: http://infomobile.w2eu.net/2011/05/24/igoumenitsa-mountain-jungles-threatened-by-eviction/.

für die Dauer von etwa einer Woche ins Gefängnis von Paganì gebracht worden. Wie alle anderen habe man ihn dort befragt, fotografiert und „gefingert". – „Fingered", so lautet der Begriff im international english, der Zirkulationssprache der neu angekommenen MigrantInnen am Berg untereinander über die Communities hinweg oder mit Leuten wie uns. Alle anderen, die mit ihm in Paganì gewesen waren, seien auf Papier gefingert worden, so Rastaman. Er auch. Er wisse nicht warum, vielleicht weil seine Abdrücke nicht scharf genug geworden seien, auf jeden Fall hätte er seine Finger auch in eine kleine Maschine mit einer Glasplatte halten müssen. Er sagt, er wisse, dass nicht alle Fingerabdrücke eine Rolle spielen. Er kenne zwei Sudanesen vom Berg, die es vor einer Woche über die Adria und dann bis nach Deutschland geschafft hätten. Und offensichtlich hätte es in Deutschland kein Problem mit ihren Fingerabdrücken gegeben. Er denke und wisse aus vielen Gesprächen und zahlreichen Erfahrungen, dass der Umgang der Griechen mit dem „fingering" nicht so genau sei. Rastaman will nach England, wo er Freunde und Familie hat. Seine Augen sind auf den Hafen gerichtet. Er wartet auf den richtigen Moment. Es gebe immer wieder Leute, die es schafften. Wenn man vom Berg weggeht, schreibt man seinen Namen und seine Telefonnummer auf die Betonwand an der Brücke zum Hafen.

Schluss

Der Hinweis darauf, dass das Glas gefährlich sei, begegnete uns im Feld wiederholt. Er scheint Teil des unter MigrantInnen zirkulierenden Wissens[10] zu sein, dessen Gültigkeit auch von den zahlreichen ExpertInneninterviews, die wir geführt haben, nicht unbedingt entkräftet wurde – z.B. in der Eurodac Central Unit in Athen und Rom.[11] Vielmehr scheinen uns die migrantischen Geschichten um das Glas ein Beleg dafür zu sein, dass die Migration ein selbstreflexiver Teil des Informations- und Kontrollkontinuums darstellt, welches – um mit Dennis Broeders (2011: 59) zu sprechen – immer zwei Modi der Exklusion umfasst: die Exklusion von der Registrierung bzw. Dokumentation und die Exklusion durch Registrierung bzw. Dokumentation. Die Modulation dieser beiden Verfahren der Exklusion bzw. deren flexibles und bewegliches Wechselspiel bildet Konjunkturen der „digital deportability" heraus. Dieser Begriff bezeichnet die Ausweitung der Risiken der Mobilität – Geld, Ausdauer, Länge des Unterwegs-Seins und manchmal das Leben selbst – auf den gesamten von der Schengener Grenze eingefassten Raum und darüber hinaus. Es handelt sich hierbei um eine Verflüssigung der europäischen Grenze, mit der Folge, dass die Deportabilität im glatten Raum der Daten-Fluidität ubiquitär wird. In diesem Raum zirkulie-

10 Zum Wissen der Migration als Teil von „mobile commons" siehe Papadopoulos/Tsianos. i.E.

11 Ausführlicher zu diesem Aspekt: Tsianos/Kuster/Kambouri/Parsanoglou, „Doing border by means of data bodies in Eurodac", Beitrag auf der XI. BRIT Konferenz „Mobile borders/Les frontières mobiles", 6.-9. September 2011, Genf.

ren allerdings nicht die MigrantInnen selbst, sondern die verkörperte Identität der Migration als Summe der „data bodies“ von MigrantInnen.[12] Eurodac-Datenkörper sind algorithmisch gewandelte Fingerabdruckprofile, welche Personen und ihre Reisestrecken innerhalb von Schengen visualisieren (statt abbilden) und projizieren (statt repräsentieren). Sie machen die mobilen und flüchtigen Körper der MigrantInnen, die sie inskribieren, nicht nur maschinen-lesbar und verifizierbar, sondern auch fluid und hypermobil. Die verkörperte Identität der Migration entspricht somit im Sinne von Latours Konzept der „unveränderlich mobilen Dinge“ dem Versuch, etwas zu verflüssigen und stillzustellen, was bisher nicht flüssig und konstant war: das Beharrungsvermögen und die Dynamik von Körpern, Dingen und Belangen in der Migration. Wie wir gesehen haben, aktivieren die „data bodies“ als zirkulierende Referenz Hin- und Rück-Beziehungen mit den MigrantInnen, die im europäischen Raum unterwegs sind und steigern so die Mobilität und die Unveränder-

12 „Data body“ ist ein Begriff, den das Critical Art Ensemble in seinem Buch „The flesh machine“ (1998) zum ersten Mal geprägt hat und dort definiert als die Gesamtheit der Sammlung von Akten oder Dateien über ein Individuum im Dienste von Unternehmen oder dem polizeilichen Staat (145). Der Bedeutungshorizont dieses Begriffs scheint uns allerdings von Vorstellungen und tatsächlichen Verarbeitungsvorgängen von personenbezogenen Daten in Großrechenzentren durch die Regierung oder durch große Firmen, wie sie in den 1970er Jahren aufgekommen sind, inspiriert. Unserer Ansicht nach müsste die Vorstellung von „data bodies“ – insbesondere, was Fragen des Datenschutzes anbelangt – für die neuen Umstände in der Informationsgesellschaft und deren Herausforderungen aktualisiert werden.

barkeit ihrer Spuren. Folgen wir Bruno Latour, ist hierbei nicht das Medium – also der biometrische Fingerabdruck[13] oder die digitale Datenbank – das Entscheidende; vielmehr geht es um die zunehmende Genauigkeit, die bei der Entsprechung von zwei Fingerabdrücken durch die Mobilisierung und die Unveränderbarkeit von Fingerbildern der Migration erzielt wird (Latour 1986). Das Konzept der unveränderlich mobilen Dinge unterscheidet sich somit markant von einer semiotischen oder medientheoretischen Herangehensweise und akzentuiert mit Blick auf die agonistische Situation oder, wie sich für unseren Fall sagen ließe, auf die Kontroverse zwischen der Migration und ihrer Kontrolle, eine Verschiebung vom Medium zur Botschaft und zum Kontext, in dem Inskriptionen einen Unterschied machen. Gerade deswegen lässt sich umgekehrt aber auch herausstellen, dass die MigrantInnen, weil sie die Grenze selbst auf ihrem Körper mit sich tragen, die Grenze also verkörpern – insbesondere auch in Form ihrer eigenen Finger –, die sie nicht vollständig zu überqueren vermögen. Vielmehr tragen sie die Grenze zugleich mit sich, wie sie dagegen ver-

13 Hierzu gilt es allerdings zu sagen, dass sich der biometrische Marker, der als ultimativer, universell anwendbarer und nahezu unfehlbarer Garant für Identität gilt, aus zwei Annahmen zusammensetzt: Zum einen die von der Empirie gestützte Annahme, dass Fingerabdrücke einzigartig sind und sich im Verlaufe des Lebens nicht verändern und zum anderen die Annahme, dass zwei identische Weisen, eine Repräsentation des Fingerabdrucks zu erzeugen, zu identischen Resultaten führen müssten. Ein Hit aufgrund der Identität von zwei Fingerabdrücken in der Eurodac-Datenbank verleiht darüber hinaus auch den weiteren, hier gespeicherten Daten, wie etwa dem Geschlecht, zusätzliche Authentizität und Glaubwürdigkeit.

stoßen. Erst auf diese Weise – als Missachtung oder als mit Füssen vollzogener Fehltritt – re-territorialisieren sie die Grenze. Sie operieren tiefer im europäischen Territorium und fordern die Grenzen Europas heraus.

Literatur

Aus, Jonathan P., 2006: Eurodac: A Solution Looking for a Problem? Working Paper No. 9, Arena. Centre for European Studies, University of Oslo.

Aus, Jonathan P., 2003: Supranational Governance in an ‚Area of Freedom, Security and Justice': Eurodac and the Politics of Biometric Control, SEI Working Paper No 72, ARENA, University of Oslo.

Broeders, Dennis, 2011: A European ‚Border' Surveillance System under Construction. In: H. Dijstelbloem and A. Meijer: Migration and the New Technological Borders of Europe, Basingstoke: Palgrave Macmillan, pp. 40-67.

Critical Art Ensemble, 1998: The flesh machine, New York, Autonomedia.

Latour, Bruno, 1986: Visualization and Cognition: Thinking with Eyes and Hands. In: Knowledge and Society: Studies in the Sociology of Culture Past and Present, Volume 6, pp. 1-40.

Latour, Bruno 2006, Drawing Things Together. Die Macht unveränderlich mobiler Elemente. In: Belliger, Andréa/Krieger, David J. (Hg.), ANThology. Ein einführendes Handbuch zur Akteur-Netzwerk-Theorie. Bielefeld, S. 257-307.

Papadopoulos, Dimitris and Vassilis Tsianos (forthcoming): After citizenship: Autonomy of migration, organizational ontology, mobile commons, In: Citizenship Studies.

Pieper, M., Kuster, B., Tsianos, V., 2011: ‚Making Connections'. Skizze einer net(h)nografischen Grenzregimeanalyse. In: O. Leistert and T. Röhle (eds.): Generation Facebook. Über das Leben im Social Net, Bielefeld, pp. 221-248.

Rabinow, P., 2003, Anthropos Today: Reflections on Modern Equipment, Princeton University Press.

Shields, Peter, 2010: ICTs and the European Union's Evolving Border Surveillance Architecture: A Critical Assessment. In: Observatorio Journal, 4 (1), 255-88.

Töpfer, Eric, 2008: Mobile Daten – begrenzte Kontrolle. Auf dem Weg zum europäischen Informationsverbund. In: Bürgerrechte & Polizei/CILIP, Nr. 91 (3), pp. 19-32.

Tsianos, Vassilis S., Kuster, Brigitta, 2012, Thematic Report „Border Crossings, http://www.mignetproject.eu/?cat=5.

Van der Ploeg, I., Sprenkels, I., 2011: Migration and the Machine-Readable Body: Identification and Biometrics. In: H. Dijstelbloem and A. Meijer (eds.) Migration and the New Technological Borders of Europe, Basingstoke: Palgrave Macmillan, pp. 68-105.

Van der Ploeg, I., 2005: The Politics of Biometric Identification. Normative aspects of automated social categorization. In: Biometric Technology & Ethics, BITE Policy Paper no. 2.

Transparenz und Datensparsamkeit von elektronischen Ausweisdokumenten in Deutschland

Transkript

Dominik Oepen

Einleitung

Von offizieller Stelle wird häufig betont, dass die Ausweisdokumente, die wir hier in Deutschland haben, einen hohen Standard an Datensicherheit, aber auch Garantien, was die Privatsphäre der Ausweisinhaber und die Transparenz angeht, haben (Bender et al. 2008, Rossnagel et al. 2008, Quiring-Kock 2009). Ich möchte heute darauf eingehen, welche technischen Mechanismen verwendet werden, um diese angeblichen Eigenschaften zu realisieren, was diese Techniken tatsächlich erreichen können und wo die Grenzen davon liegen.

Dazu gebe ich zunächst eine kurze Einführung in elektronische Ausweisdokumente. Das ist ein sehr breites Thema, darum werde ich das vergleichsweise kurz abhandeln müssen. Der Fokus liegt dann auf den Ausweisdokumenten, die hier in Deutschland tatsächlich eingeführt wurden. Das sind drei Stück: der elektronische Reisepass (ePass), der neue Personalausweis (nPA) und der elektronische Aufenthaltstitel (eAT). Der Fokus soll auf der Technik liegen, die zum einen Zugriffsschutz implementiert, zum anderen Mechanismen, die eine möglichst datensparsame Nutzung gewährleisten sollen.

Wenn man über elektronische Ausweisdokumente spricht, dann gibt es sehr viele Gremien und Institutionen, die an der Standardisierung beteiligt sind, aber man kann sicherlich sagen, dass auf internationaler Ebene eine der wichtigsten Institutionen die ICAO ist. ICAO steht für International Civil Aviation Organisation. Das ist eine Institution, die es bereits seit den fünfziger Jahren gibt und die bereits seit den achtziger Jahren Standards für maschinenlesbare Reisedokumente entwirft. Das zentrale Dokument ist dabei das ICAO-Dokument 9303 (ICAO 2008, ICAO 2008a), welches die sogenannten *Machine Readable Travel Documents* spezifiziert und welches mittlerweile von einer Vielzahl von Ländern adaptiert wird. Ich hatte jetzt die Zahl über 100 Länder gefunden, wir haben vorhin schon gehört, es sind jetzt 191 Länder. Vielleicht sind es dann mittlerweile auch mehr als 300 Millionen Passdokumente, die bisher weltweit ausgegeben wurden. Man kann auf jeden Fall sehen, dass der Standard weit verbreitet ist.

Maschinenlesbar bedeutete damals nicht unbedingt auf elektronischem Weg maschinenlesbar, sondern in den achtziger Jahren bedeutete dies zunächst einmal optisch lesbar. Vielleicht kennen Sie alle die maschinenlesbare Zone (*Machine Readable Zone*, MRZ) aus Ihrem Reisepass: Das sind drei Zeilen unten in Ihrem Reisepass, die in einem standardisierten Format, in einer maschinenlesbaren Schrift Informationen über den Passinhaber enthalten.

Nach den Terroranschlägen am 11. September hat sich relativ schnell etabliert, dass das optische Auslesen nicht mehr reicht, sondern es wurde im Mai 2003 der Beschluss

gefasst, die Dokumente nicht mehr nur auf optischem Wege verarbeitbar zu machen, sondern jetzt eben auch auf elektronischem Wege. Zu diesem Zweck sollten RFID-(Radio-Frequency-Identification-)Chips in den Pässen verbaut werden und auf diesen Chips sollten – neben den aufgedruckten Daten – auch biometrische Daten der Passinhaber gespeichert werden. Dabei waren zunächst ein digitales Gesichtsbild vorgesehen, optional aber auch Fingerabdrücke, Irisscans und es sind auch noch weitere biometrische Merkmale spezifiziert.

RFID ist ein schwieriger Begriff, weil das eine ganze Palette an Technologien umfasst, die teilweise recht unterschiedliche Eigenschaften haben. Im Rahmen elektronischer Ausweisdokumente sprechen wir eigentlich immer von dem ISO-Standard 14443 (ISO 14443-4 2000), das ist eine Nahfunktechnologie, die bei spezifikationskonformem Betrieb Reichweiten von ungefähr fünf bis zehn Zentimetern erreicht. Es wurden natürlich schon viele Untersuchungen angestellt, ob man diese Reichweite nicht eventuell vergrößern kann, um beispielsweise unberechtigten Zugriff auf einen Ausweis oder Reisepass zu erhalten. Nach meinem Kenntnisstand ist da der Stand der Forschung so, dass in Modellierung und Simulation Reichweiten von 40 bis 50 Zentimetern vorausgesagt werden (Kfir/Wool 2005), die erreicht werden können und in der Praxis ist der Rekord bei etwa 25 Zentimetern (Finke/Kelte 2004, Kirschenbaum/Wool 2008). Das war jetzt 2006, eventuell gibt es da schon neuere Erkenntnis-

se, dass man noch näher an die 40 Zentimeter rankommt, aber ich glaube, über einen halben Meter ist bisher noch niemand hinausgekommen.

Das gilt allerdings nur für das aktive Ansprechen eines Chips; wenn man versucht, aktiv eine Verbindung zu einem Ausweis aufzubauen, dann kann man das ungefähr über diese Reichweite schaffen. Das passive Abhören geht technologiebedingt über sehr viel weitere Entfernungen. Also, wenn ich eine bestehende Kommunikation mit einem Dokument und einem Lesegerät belauschen möchte, dann geht das auch über eine Entfernung von mehreren Metern.

Elektronische Ausweisdokumente in Deutschland

Die Einführung elektronischer Reisedokumente in Deutschland erfolgte schrittweise. Bereits vor der Einführung des ersten Dokuments, des elektronischen Reisepasses, wurde die sogenannte eCard-Strategie des Bundes beschlossen (BMWi, Kowalski 2007). In diesem Strategiepapier hat die Bundesregierung festgeschrieben, dass sie die Verbreitung von Chipkarten in allen Bereichen von eBusiness und eGovernment stark fördern möchte und dass sie vor allem elektronische Authentisierungsdienste und elektronische Signaturdienste fördern möchte. In diesem Strategiepapier wurden dann beispielhaft einige Chipkarten, wie etwa die Jobkarte, ELENA, die elektronische Gesundheitskarte, ELSTER und der elektronische Personalausweis, als wegweisende Projekte aufgeführt.

Man kann an dieser Stelle schon sehen, dass nicht unbedingt alle diese Dokumente erfolgreich eingeführt wurden.

Was allerdings erfolgreich eingeführt wurde, ist der elektronische Reisepass. Wie wir das vorhin schon gehört haben,[1] ist das in zwei Phasen erfolgt: Im November 2005 wurde der Reisepass mit Chip eingeführt. Damals waren auf dem Chip noch keine Fingerabdrücke abgespeichert, sondern lediglich das digitale Gesichtsbild und die aufgedruckten Daten. Erst im November 2007 wurde dann die Abspeicherung von zwei Fingerabdrücken verpflichtend. Nachfolgend wurden dann im November 2010 der neue Personalausweis eingeführt und im September 2011 der elektronische Aufenthaltstitel. Und diese drei Dokumenttypen möchte ich jetzt im Detail beleuchten.

Zum elektronischen Reisepass haben wir eigentlich schon alles gehört, daher dazu nur relativ kurz: Er ist ein Ausweisdokument, welches genau eine Applikation bietet, nämlich die ePass-Applikation. Diese Applikation ist dafür gedacht, mich an der Grenze auszuweisen, beziehungsweise ist der Zugriff allgemein für hoheitliche Zwecke vorgesehen, also für Polizeibeamte, für Zoll- und Grenzbeamte, etc. Innerhalb der ePass-Applikation sind drei Datengruppen gespeichert: die maschinenlesbare Zone ist nochmal digital gespeichert, außerdem das biometrische Gesichtsbild und in der Datengruppe Drei die Fingerabdrücke des Ausweisinhabers. Darüber hinaus sind kryptografische Signaturen gespeichert für alle Datengruppen, die dafür dienen sicherzustellen, dass die

1 Im Vortrag von Frau Hansen (zusammengefasst Seite 73).

Daten, die ausgelesen werden, auch tatsächlich authentisch sind. Auf diese Authentizitätssicherung gehe ich später noch im Detail ein.

Der neue Personalausweis bietet dagegen mehr als nur eine Funktion. Genauer gesagt sind es drei Applikationen, die auf dieser Karte laufen: Das sind die ePass- oder Biometrie-Applikation, die im wesentlichen kompatibel ist zu der Applikation, die wir aus dem elektronischen Reisepass kennen, dann die eID-Applikation, die konzipiert wurde, um die Authentisierung des Ausweisinhabers über das Internet zu realisieren – vor allem über das Internet. Es waren auch mal Automaten für Zigarettenkauf oder ähnliches im Gespräch, aber der Hauptanwendungszweck waren auf jeden Fall immer eBusiness- und eGovernment-Anwendungen über das Internet. Und die dritte Applikation ist die eSign-Applikation zur Erstellung von qualifizierten elektronischen Signaturen (BSI 2012b). Man sieht, wie sich die eCard-Strategie widerspiegelt in diesem Dokument: Es sollten elektronische Authentisierung und Signaturfunktionen gefördert werden und deshalb wurden genau diese Funktionen jetzt auch auf dem Ausweisdokument untergebracht. Wichtig ist es jetzt anzumerken, dass es bei der ePass-Applikation dann doch einen kleinen Unterschied zum Reisepass gibt, nämlich, dass die Speicherung der Fingerabdrücke optional ist. Als Ausweisinhaber muss ich mich bei der Beantragung des Ausweises entscheiden, ob ich Fingerabdrücke abgeben möchte oder nicht und kann eben auch gezielt darauf verzichten. Genauso optional sind die eID-Applikation und die eSign-Applikation. Auch hier kann ich bei der Bean-

tragung des neuen Personalausweises sagen, ich möchte die eID-Applikation nicht nutzen; die eSign-Applikation muss eh erst durch das Nachladen eines Zertifikates nutzbar gemacht werden. Ich kann auch zu einem späteren Zeitpunkt die eID-Applikation freischalten lassen, wenn ich mich zuerst dagegen entschieden habe oder sie deaktivieren lassen, wenn ich sie zuerst habe aktivieren lassen. Das sind allerdings kostenpflichtige Vorgänge.

Datengruppe	Inhalt
DG 1	Dokumenttyp
DG 2	Ausgebender Staat
DG 3	Ablaufdatum
DG 4	Vorname(n)
DG 5	Familienname
DG 6	Ordensname/Künstlername
DG 7	Doktorgrad
DG 8	Geburtsdatum
DG 9	Geburtsort
DG 13	Geburtsname
DG 17	Adresse
DG 18	Wohnort ID

Tabelle 1

Datengruppen der eID-Applikation

Schauen wir uns nun die Datengruppen der eID-Applikation an. Die sind hier (Tabelle 1) aufgelistet. Es sollte eigentlich größtenteils verständlich sein, was die einzelnen Datengruppen bedeuten.

Wichtig ist es hierbei festzuhalten, dass ein Dienst, bei dem ich mich als Ausweisinhaber anmelde, nicht per se auf alle diese Daten zugreifen kann. Wir werden nachher sehen, dass der Dienstanbieter zur Nutzung dieser Funktion ein sogenanntes Dienstanbieterzertifikat benötigt und in diesem Zertifikat ist festgeschrieben, welche Daten der Dienstanbieter auslesen darf. Er ist also beschränkt in seinem Zugriff auf die eID-Applikation und kann nicht alle Daten über den Nutzer erfassen, sondern nur diejenigen, für die er vorher bei der Beantragung des Zertifikates glaubhaft machen konnte, dass es für die Erbringung seines Dienstes zwingend notwendig ist, dass er diese Daten erhebt. Dafür gibt es die neu geschaffene Vergabestelle für Berechtigungszertifikate beim Bundesverwaltungsamt und wenn ich die eID-Funktion als Dienstanbieter nutzen möchte, muss ich zunächst einmal glaubhaft machen, dass ich für meinen Geschäftszweck gewisse Daten zwingend erheben muss. Hier sehen wir die Datensparsamkeits- und Transparenzaspekte, die beim neuen Personalausweis eine Rolle spielen. Jetzt kann man natürlich spekulieren, wie gut diese Prüfung erfolgt; es gibt da so einige Dienste in der freien Wildbahn, bei denen man sich so fragt: Wie sind denn die damit durchgekommen? Aber prinzipiell dürfen nur die jeweils notwendigen Daten erhoben werden.

Ein interessantes Detail gibt es dazu noch: Nämlich gelten diese Einschränkungen lediglich für Dienstanbieter aus der Privatwirtschaft. Als Dienstanbieter muss ich also belegen, auf welche Daten ich zugreifen darf. Inspektionssysteme, also solche Terminals, die eigentlich

für den Grenzübergang gedacht sind, können die Berechtigung zum kompletten Zugriff auf die Applikation erhalten. Das heißt, ein Grenzkontrollsystem hat auf einmal nicht mehr nur noch Zugriff auf die Passapplikation, sondern zusätzlich noch auf die in der eID-Applikation abgespeicherten Daten.

Ein weiteres technisches Detail ist, dass in der eID-Applikation – im Gegensatz zur ePass-Applikation – keine Signaturen gespeichert sind. Der Grund dafür ist, dass man verhindern wollte, dass Dienstanbieter Daten, welche aus einem Ausweis ausgelesen wurden, weiterverkaufen können. Sie können ohne diese Signaturen nämlich nicht glaubhaft machen, dass es tatsächlich aus einem Ausweis ausgelesene Daten sind. Hier wurde auf einen Sicherheitsmechanismus, welcher noch bei der ePass-Applikation des Reisepasses eingeführt wurde, verzichtet, um den Datenschutz in gewisser Weise zu stärken.

Neben dem Zugriff auf verschiedene Datengruppen bietet die eID-Applikation noch drei sogenannte spezielle Funktionen, die ebenfalls entworfen wurden, um Dienste mit einem möglichst hohen Maß an Datensparsamkeit implementieren zu können. Hierbei handelt es sich um die *Restricted Identification*, die *Altersverifikation* und die sogenannte *Wohnort-ID*. Die Restricted Identification dient dazu, dass sich ein Ausweisinhaber pseudonym bei einem Dienst anmelden kann, ohne dass mehrere Dienste miteinander kooperieren können, um denselben Ausweisinhaber dienstübergreifend zu tracken. Man kann sich das mit einem Beispiel veranschaulichen: Wenn ich mich mit meinem Personalausweis bei Amazon und bei

der Schufa anmelde, dann erhalte ich verschiedene Pseudonyme bei diesen Diensten und die Dienste können nicht miteinander kooperieren, um herauszufinden, dass ich dieselbe Person bin. Es bleibt hier außen vor, dass es natürlich weiterhin andere Möglichkeiten gibt, den Nutzer zu verfolgen. Das Ziel war es, mit der Onlineauthentisierung keine neuen Mechanismen zum Nutzertracking zu bieten und einmal exemplarisch zu versuchen, das Ganze so datensparsam wie möglich zu realisieren. Es gibt pro Kombination aus Ausweisinhaber und Dienstanbieter genau ein Pseudonym, es ist also eindeutig für die Kombination aus Ausweis und Dienst, aber nicht verkettbar, wir haben also hier die Unlinkability, die wir vorhin[2] vorgestellt bekommen haben.

Die Altersverifikation dient dazu, Dienste anzubieten, die nur für eine bestimmte Altersgruppe zugänglich sein sollen – also beispielsweise Dienste, die erst ab 16 oder 18 zugänglich sein sollen –, ohne das tatsächliche Alter des Ausweisinhabers zu erheben. Der Dienst übermittelt dazu ein Referenzdatum an den Ausweis und der Ausweis antwortet: „Ja, der Ausweisinhaber ist vor diesem Referenzdatum geboren“ oder „Nein, das ist nicht der Fall“. Hier geht es also wieder darum, möglichst wenig Daten zu erheben. Die Informatikerfrage ist üblicherweise: „Was ist, wenn man mehrere Anfragen stellt? Kann man dann nicht möglicherweise doch relativ schnell das tatsächliche Alter herausfinden?“ Da ist die Antwort, dass pro Durchlauf des Protokolls genau eine Anfrage gestellt werden kann.

2 Ebenfalls im Vortrag von Frau Hansen (zusammengefasst Seite 73).

Ähnlich ist es mit der Wohnort-ID. Hier sollte ermöglicht werden, Dienste für einen bestimmten Bezirk bzw. für ein bestimmtes geographisches Gebiet zugänglich zu machen, ohne den tatsächlichen Wohnort des Ausweisinhabers erfassen zu müssen. Wieder ist es so, dass ein Referenzdatum an den Ausweis übermittelt werden kann – beispielsweise: „Wohnt der Ausweisinhaber in Brandenburg?" – und dann kommt die Antwort Ja oder Nein zurück. Grundlage dafür ist der sogenannte amtliche Gemeindeschlüssel, welcher verschiedene Auflösungsstufen, wie etwa Gemeinde, Region, Bundesland, vorsieht.

Das neueste elektronische Ausweisdokument in Deutschland ist der elektronische Aufenthaltstitel. In Deutschland benötigen Ausländer aus dem Nicht-EU-Ausland, die ihren ständigen Wohnsitz in Deutschland haben, einen Aufenthaltstitel. Früher waren das einfach Aufkleber in den nationalen Reisepässen der Migranten. Das wurde 2011 ersetzt durch den elektronischen Aufenthaltstitel, ebenfalls eine Chipkarte, die von der Technik sehr stark angelehnt ist an den neuen Personalausweis. Von der Funktionalität sind der nPA und der elektronische Aufenthaltstitel beinahe identisch, es sind auch wieder ePass-Applikation, eID-Applikation und eSign-Applikation vorhanden. Die Dokumente unterscheiden sich dann aber im Detail doch. Ein wichtiger Unterschied ist sicherlich, dass für den elektronischen Aufenthaltstitel die Speicherung der Fingerabdrücke verpflichtend ist, nicht wie beim neuen Personalausweis optional. Besonders interessant ist das in dem Kontext, dass er auch von Kindern ab sechs Jahren benötigt wird, also auch Kinder,

die als Ausländer ihren Wohnsitz in Deutschland haben, müssen ihre Fingerabdrücke abgeben. Wir haben ja vorhin[3] schon gehört, dass das nicht immer so sinnvoll ist, da sich bei Kindern doch noch einiges verändert im Laufe der Zeit, aber so ist der Stand. Kleine Unterschiede sind dann noch, dass die eID über zusätzliche Datengruppen verfügt und, ich glaube, auch einige der Datengruppen aus der eID-Applikation des Personalausweises nicht vorhanden sind. Die Staatszugehörigkeit und verschiedene Nebenbestimmungen zum Aufenthalt sind innerhalb dieser Applikation gespeichert.

Transparenz und Privatsphäre

Soviel zur Funktionalität der Ausweisdokumente in Deutschland, jetzt möchte ich versuchen, den Zugriffsschutz zu erklären. Der elektronische Reisepass implementiert die sogenannte *Extended Access Control* (EAC) nach Version 1, welche in dem eingangs erwähnten ICAO-Dokument 9303 spezifiziert ist. Der Zugriffsschutz lässt sich in zwei Phasen aufgliedern, die sogenannte *Basic Access Control* (BAC) und die *Active Authentication*, welche wiederum aus zwei Protokollen, der *Chip Authentication* (CA) und der *Terminal Authentication* (TA), besteht. Im Rahmen der Basic Access Control wird ein verschlüsselter Kanal aufgebaut zwischen Terminal und Ausweisdokument. Die Grundlage dafür ist wieder die maschinenlesbare Zone: der Ausweis wird optisch eingelesen, auf der Basis der maschinenlesbaren Zone werden zwei symmetrische Schlüssel abgeleitet. Mit diesen

3 Im Vortrag von Prof. Dr. Miloš Vec (zusammengefasst Seite 63).

beiden Schlüsseln kann ich auf die Datengruppen Eins und Zwei zugreifen, also auf das Gesichtsbild und auf die maschinenlesbare Zone. Die Durchführung der Basic Access Control wird häufig mit dem Vorzeigen des Ausweisdokuments verglichen. Das bedeutet, ich muss die maschinenlesbare Zone kennen, um auf die elektronischen Funktionen des Reisepasses zugreifen zu können. Ich muss also schon einmal die codierten Daten optisch eingelesen haben, um sie anschließend noch einmal elektronisch lesen zu können. Zusätzlich erhalte ich Zugriff auf das digitale Gesichtsbild.

Bei der BAC handelt es sich um einen rein symmetrischen Vorgang, die weiteren Protokollschritte sind asymmetrisch. Mit der Chip Authentication wird die Authentizität des Reisepasses nachgewiesen. Der Reisepass weist also nach, dass es sich um einen echten Pass handelt, indem er ein asymmetrisches Schlüsselpaar, welches nicht-auslesbar im Chip des Reisepasses gespeichert ist, verwendet. In die andere Richtung weist das Terminal nach, dass es tatsächlich berechtigt ist, auf den Reisepass zuzugreifen. Dafür benötigt es ein sogenanntes Terminalzertifikat, welches unter bestimmten Bedingungen ausgestellt wird, und natürlich den zugehörigen Schlüssel. Wir haben hier also eine beidseitige Authentifizierung zwischen Terminal und Reisepass, jeweils auf der Grundlage asymmetrischer Kryptografie, und erst danach ist der Zugriff auf die Fingerabdrücke möglich. Die Active Authentication ist also nochmal ein zusätzlicher Schutz der Fingerabdrücke, die im elektronischen Reisepass gespeichert sind.

Für den neuen Personalausweis hat das Bundesamt für Sicherheit in der Informationstechnik Änderungen an dem Zugriffsschutz vorgenommen und dafür die Technische Richtlinie 3110 erstellt. In dieser technischen Richtlinie ist die Extended-Access-Control-Version 2 spezifiziert (BSI 2012a). Hier gibt es die Basic Access Control nicht mehr. Sie wurde durch ein neues Protokoll ersetzt, das sogenannte *Password Authenticated Connection Establishment* (PACE). Dieses Protokoll dient wieder zur Absicherung der Funkschnittstelle: Es soll vermeiden, dass Leute, die sich in Funkreichweite befinden, die Kommunikation zwischen Ausweis und Terminal abhören. Deswegen wird ein verschlüsselter Kanal zwischen der Stelle der PIN-Eingabe und dem Personalausweis aufgebaut.

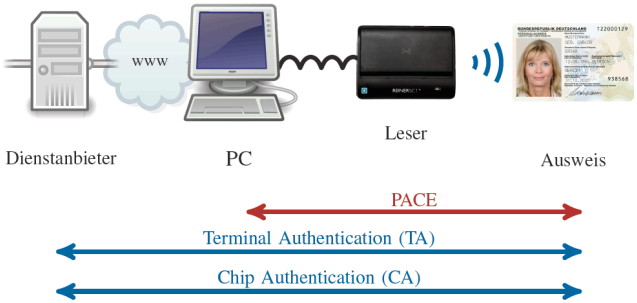

Abbildung 1 – EAC am Beispiel der eID-Funktion mit einem Basisleser

Wenn ich ein Lesegerät mit eigener Tastatur verwende, dann wird der PACE-Kanal zwischen dem Lesegerät und dem Personalausweis aufgebaut und wenn ich ein Lese-

gerät ohne eigene Tastatur verwende, dann wird der Kanal zwischen dem Computer und dem Ausweis aufgebaut.

Was man hier noch sieht, ist, dass die Reihenfolge von Terminal Authentication und Chip Authentication im Vergleich zur beim Reisepass verwendeten EAC-Version 1 umgedreht wurde. Jetzt muss zunächst der Dienstanbieter, bzw. das Inspektionssystem, nachweisen, dass es zum Zugriff auf den Personalausweis berechtigt ist, bevor der Ausweis seine Authentizität nachweist. Wenn man die beiden Versionen der EAC miteinander vergleicht, dann kann man vermuten, dass das BSI versucht hat, die Kritik, die an der ersten Version der EAC geäußert wurde, beim nPA zu entkräften. Man sieht, dass genau an den Stellen, die zuvor häufig kritisiert wurden, Änderungen vorgenommen wurden. Die BAC stand zuvor recht stark im Fokus von Sicherheitsuntersuchungen (Liu et al. 2007, Hoepman et al. 2006, Carluccio et al. 2007). Es wurde argumentiert, dass die abgeleiteten Schlüssel nicht ideal sind und nicht über ausreichend Entropie verfügen, dass es keinen Sicherheitsbeweis für das Protokoll gibt, dass teilweise die maschinenlesbaren Zonen zur Ableitung der symmetrischen Schlüssel in einigen Ländern vorhersagbar sind und man daher die benötigten Schlüssel erraten kann. All diese Kritik sollte nun entkräftet werden, indem ein neues Protokoll mit einem zugehörigen Sicherheitsbeweis innerhalb eines bestimmten kryptografischen Modelles entwickelt wurde.

Außerdem wurde, wie bereits erwähnt, die Reihenfolge von CA und TA vertauscht. Zuvor wurde kritisiert, dass ein Chip, welcher sich vor dem Terminal authentisiert, diese Authentisierung evtl. gegenüber einem Terminal, welches gar nicht zum Zugriff berechtigt ist, ausführt. Das würde eventuell das Tracken des Ausweises erlauben. Jetzt ist es so, dass sich zuerst das Terminal gegenüber dem Ausweis ausweisen muss und dafür ein Zertifikat, welches es zum Zugriff auf den Ausweis berechtigt, vorweisen muss. Erst danach weist sich der Ausweis gegenüber dem Terminal aus. Dahinter steht die kryptografische Best Practice, dass sich zuerst die stärkere von zwei Parteien authentisieren sollte.

Ein weiterer wichtiger Unterschied zum elektronischen Reisepass ist, dass beim nPA kein Zugriff auf die im Ausweis gespeicherten Nutzdaten möglich ist, ohne die komplette EAC durchzuführen.[4] Erst nach der Durchführung von PACE, TA und CA können Daten vom Personalausweis ausgelesen werden. Beim Reisepass hingegen reicht schon die BAC, um auf das Gesichtsbild und die aufgedruckten Daten zuzugreifen.

Interessanterweise ist der elektronische Aufenthaltstitel zur EAC-Version 1 abwärtskompatibel, obwohl er nach dem nPA eingeführt wurde. Der elektronische Aufenthaltstitel unterstützt also für die ePass-Applikation sowohl das neue PACE-Protokoll als auch das alte BAC-Protokoll. Weiterhin ist es hier auch wieder möglich, bereits nach BAC die aufgedruckten Daten auszule-

4 Es ist allerdings möglich, auf dem Funkweg zu erkennen, dass es sich um einen neuen Personalausweis handelt.

sen. Das bedeutet, es wurde zunächst für den neuen Personalausweis ein stärkeres Verfahren entwickelt, dann aber für den Aufenthaltstitel – aufgrund von Abwärtskompatibilität und aufgrund von internationalen Bestimmungen – doch wieder das schwächere, ältere Verfahren beibehalten. Man kann also sagen, dass die Inhaber von neuen Personalausweisen besser geschützt sind als die Inhaber von elektronischen Aufenthaltstiteln.

Für die eID-Funktion sind noch weitere Funktionen verbaut, die ein möglichst hohes Maß an Transparenz gewährleisten sollen. Es ist vorgeschrieben, dass im Rahmen der Terminal-Authentisierung dem Ausweisinhaber zunächst einmal Informationen zum Dienstanbieter angezeigt werden müssen und er auch noch einmal eine Kontrolle über die Daten, die ausgelesen werden sollen, hat.

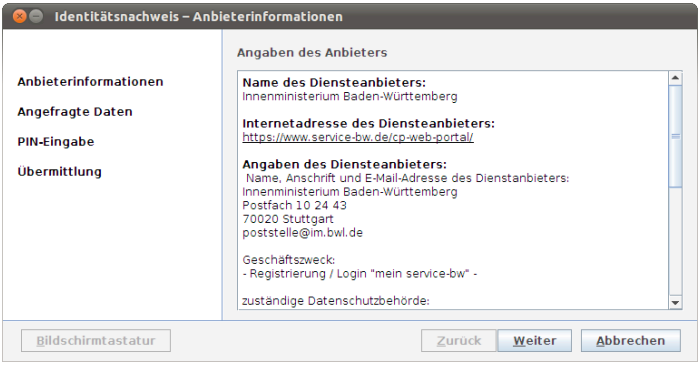

Abbildung 2 – Anzeige der Informationen zum Dienstanbieter

Besonders interessant ist, dass im nächsten Schritt angezeigt wird, auf welche Daten der Dienstanbieter zugreifen darf und dass der Ausweisinhaber die Möglichkeit hat, diese Zugriffsberechtigungen noch einmal einzuschränken. Wenn ein Anbieter jetzt also auf meinen Namen und Nachnamen zugreifen darf, ich aber meinen Nachnamen nicht freigeben möchte, dann kann ich gezielt diese Berechtigung abwählen.

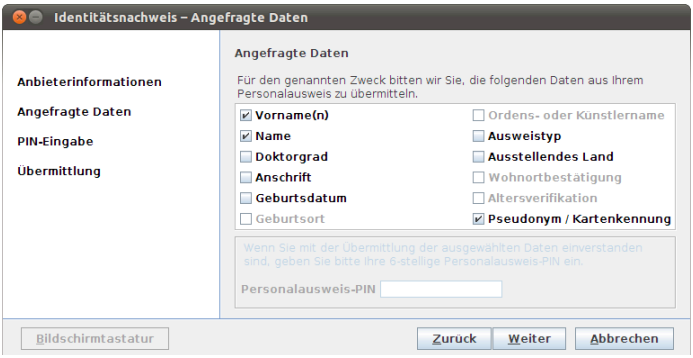

Abbildung 3 – Möglichkeit zur Abwahl von Zugriffsrechten durch den Benutzer

Natürlich kann der Dienstanbieter den Dienst anschließend verweigern. Insofern ist das nicht immer eine wirksame Maßnahme, aber die Mechanismen, die wir vorhin vorgestellt bekommen haben,[5] vor allem die Nutzerkontrolle über die erhobenen Daten, sind hier umgesetzt. Auch das gilt allerdings nur für die eID-Funktion. Bei der Authentisierung gegenüber hoheitlichen Stellen gibt es keine Möglichkeit, die auszulesenden Daten einzuschränken.

5 Im Vortrag von Frau Hansen (zusammengefasst Seite 73).

Für die Chip-Authentisierung wird, wie bereits erwähnt, ein asymmetrisches Schlüsselpaar verwendet. Dieser asymmetrische Schlüssel könnte zur Identifizierung des Ausweisinhabers verwendet werden, man könnte also das Authentisierungsprotokoll zur eindeutigen Identifizierung des Ausweisinhabers nutzen. Das war allerdings explizit nicht gewollt. Beispielsweise soll bei der Altersverifikation der Dienstanbieter den Nutzer nicht identifizieren können, auch nicht pseudonym. Aus diesem Grund wurde die Chip-Authentisierung nicht mit einem individuellen Schlüsselpaar pro Ausweis realisiert, sondern innerhalb einer Charge von Ausweisdokumenten wird für alle Dokumente derselbe CA-Schlüssel verwendet. Eine Charge ist dabei in etwa die Anzahl an Ausweisen, die in einem Zeitraum von drei Monaten produziert wird. Das sollen in etwa eine Million Ausweise sein. Das bedeutet, dass immer etwa eine Million Ausweise denselben CA-Schlüssel beinhalten. Man hat also ein Anonymitätsset von einer Million Menschen, die denselben Schlüssel verwenden. Auch hier handelt es sich um einen Datensparsamkeitsmechanismus, der umgesetzt wurde, der dann aber auch – ich glaube, es war auf dem 26C3 hier in Berlin (Plötz 2009) – als potentieller Angriffspunkt identifiziert wurde. Die Konsequenz ist, dass ein Angreifer, der einen einzigen Schlüssel bricht, beliebige Ausweise emulieren kann. Es ist auch nicht möglich, anhand des CA-Schlüssels einzelne Ausweisdokumente zu sperren. Wir sehen also einen Trade-Off zwischen Fälschungssicherheit und Datensparsamkeit.

Nachdem dieser potenzielle Angriff vorgestellt wurde, hat das BSI reagiert und eine Datei auf dem Chip spezifiziert, das sogenannte EF.ChipSecurity, die einen zusätzlichen, chip-individuellen Schlüssel beinhaltet. Die ursprüngliche Idee der Gruppenschlüssel wurde also durch die Einführung eines zusätzlichen Schlüssels ausgehebelt. Auf diesen zusätzlichen Schlüssel haben nur sogenannte privilegierte Terminals Zugriff. Angeblich gibt es derzeit noch gar keine derartigen Terminals. Es ist aber davon auszugehen, dass sobald es Zweifel daran gibt, ob ein Schlüssel gebrochen wurde oder nicht, alle Terminals zu privilegierten Terminals gemacht werden.

In den letzten Monaten wurde verstärkt Open-Source-Software zur Verwendung des neuen Personalausweises veröffentlicht. Unter anderem wurde von der Humboldt-Universität in Kooperation mit der Bundesdruckei ein Programm zur Nutzung des nPA veröffentlicht. Auch Firmen aus der Privatwirtschaft – beispielsweise Bremen Online Services – haben solche Programme veröffentlicht. Das wird auch meistens explizit mit dem Anspruch gemacht, das Vertrauen in die Programme und das System an sich zu stärken, damit eine unabhängige Kontrolle erfolgen kann. Zuvor wurde häufig spekuliert, ob mit der AusweisApp auch gleich der Bundestrojaner ausgeliefert wird, bei einer Open-Source-Lösung kann man prinzipiell erst einmal nachgucken, ob das der Fall ist oder nicht. Aber auch da muss man einschränken, dass das kein Allheilmittel ist, dass der Transparenz durch Open Source natürlich Grenzen gesetzt sind. Ich möchte hier verweisen auf den berühmten Aufsatz von Ken Thompson,

„Reflections on trusting trust“ (Thompson 1984): Nur weil ich den Quellcode zu etwas habe, bedeutet das noch nicht, dass es tatsächlich absolut transparent ist.

Weiterhin existiert Open-Source-Software natürlich nur für die eID-Applikation, nicht für die ePass-Applikation und die Chipkarte selbst. Das Lesegerät und der eID-Server sind auch alle nicht Open Source. Ein kleiner Teil der Software ist also etwas besser kontrollierbar als vorher, aber dabei handelt es sich eben nur um einen Teil des Ökosystems. Am Schluss der Extended Access Control entsteht ein Ende-zu-Ende-verschlüsselter Kanal zwischen Dienstanbieter und Ausweis. Das bedeutet, an der Stelle hat der Ausweisinhaber keinerlei Kontrolle mehr darüber, was tatsächlich aus dem Ausweis ausgelesen wird, und muss auf die technische Spezifikation vertrauen, darauf, dass die Daten, die freigegeben wurden, tatsächlich die sind, die ausgelesen werden. In den Personalausweis selber kann man nicht reinschauen.

Fazit

Zusammenfassend kann man sagen, dass verschiedene Mechanismen implementiert wurden, insbesondere beim neuen Personalausweis, im Vergleich zu vorangegangenen Dokumenten, die klar darauf abzielen, mehr Transparenz und Datensparsamkeit zu gewährleisten, allerdings vor allem im Bereich eID. Der Bereich der hoheitlichen Authentisierung entzieht sich dem. Man hat unter anderem die kryptografischen Protokolle verbessert, hat aber gerade bei Dokumenten, die für den internationalen Grenzübergang gedacht sind, doch wieder Abwärtskom-

patibilität gefordert und kommt dadurch nicht so recht weg von den alten Spezifikationen. Es gibt starke Anstrengungen zur internationalen Standardisierung. Das BSI bemüht sich die neue Version der EAC auch auf internationaler Ebene zum Einsatz zu bringen. Es gibt bereits eine Ergänzung zum ICAO-Standard, die das PACE-Protokoll nachrüstet, aber es wird vermutlich viele Jahre dauern, bis das in die Pässe einfließt. An verschiedenen Stellen sehen wir auch eine prinzipielle Schwierigkeit, die Balance zu finden zwischen Fälschungssicherheit auf der einen und Datensparsamkeit auf der anderen Seite: zwei Aspekte, die nicht ganz einfach unter einen Hut zu bekommen sind.

Literatur

Bender, Jens, Dennis Kügler, Marian Margraf und Ingo Naumann, 2008: Sicherheitsmechanismen für kontaktlose Chips im deutschen elektronischen Personalausweis. In: Datenschutz und Datensicherheit, 3:173-177.

BMWi: Chipkarten-Strategie der Bundesregierung (eCard-Strategie).
http://www.bmwi.de/BMWi/Redaktion/PDF/E/ecard-strategie,property=pdf,bereich=bmwi,sprache=de,rwb=true.pdf.

BSI, 2012a: Advanced Security Mechanisms for Machine Readable Travel Documents. Technical Guideline 03110, Bonn, März. Version 2.10.

BSI, 2012b: Architektur Elektronischer Personalausweis. Technische Richtlinie 03127, Bonn, Oktober. Version 1.15.

Carluccio, Dario, Kerstin Lemke-Rust, Christof Paar und Ahmad-Reza Sadeghi, 2007: E-passport: the global traceability or how to feel like a UPS package. In: Information Security Applications, Seiten 391-404. Springer.

Finke, Thomas und Harald Kelte, 2004: Radio Frequency Identification – Abhörmöglichkeiten der Kommunikation zwischen Lesegerät und Transponder am Beispiel eines ISO14443-Systems. Technischer Bericht, Bundesamt für Sicherheit in der Informationstechnik.

Hoepman, Jaap-Henk, Engelbert Hubbers, Bart Jacobs, Martijn Oostdijk und Ronny Wichers Schreur, 2006: Crossing borders: Security and privacy issues of the european e-passport. In: Advances in Information and Computer Security, Seiten 152-167. Springer.

ICAO, 2008: Doc 9303 – Machine Readable Travel Documents – MRTDs with Machine Readable Data Stored in Optical Character Recognition Format. International Civil Aviation Organisation, 3. Auflage.

ICAO, 2008a: Doc 9303, Machine Readable Travel Documents, Part 3, Specifications for Electronically Enabled MRtds with Biometric Identification Capability, Band 2. International Civil Aviation Organisation, 3. Auflage.

ISO 14443-4, 2000: Identification cards – Contactless integrated circuit(s) cards – Proximity cards – Part 4: Transmission protocol. ISO/IEC.

Kfir, Ziv und Avishai Wool, 2005: Picking virtual pockets using relay attacks on contactless smartcard. In: Security and Privacy for Emerging Areas in Communications Networks, 2005. SecureComm 2005. First International Conference on, Seiten 47-58. IEEE.

Kirschenbaum, Ilan und Avishai Wool, 2008: How to build a low-cost, extended-range RFID skimmer. Dissertation, Tel Aviv University.

Kowalski, Bernd, 2007: Die eCard-Strategie der Bundesregierung im Überblick. In: D. Hühnlein, A. Brömme, E, C. Busch (Herausgeber), BIOSIG, Seiten 87-96.

Liu, Yifei, Timo Kasper, Kerstin Lemke-Rust und Christof Paar, 2007: E-passport: Cracking basic access control keys. In: On the Move to Meaningful Internet Systems 2007: CoopIS, DOA, ODBASE, GADA, and IS, Seiten 1531-1547. Springer.

Plötz, Henryk, 2009: Technik des neuen ePA. Proceedings of the 26th Chaos Communication Congress.

Quiring-Kock, Gisela, 2009: PKI für Bürger – transparent, sicher, datenschutzgerecht? Datenschutz und Datensicherheit, 7:391-395.

Rossnagel, Alexander, Gerrit Hornung und Christoph Schnabel, 2008: Die Authentisierungsfunktion des elektronischen Personalausweises aus datenschutzrechtlicher Sicht. Datenschutz und Datensicherheit, 3:168-172.

Thompson, Ken, 1984: Reflections on trusting trust. Communications of the ACM, 27(8):761-763.

Biometrische Identitäten und ihre Rolle in den Diskursen um Sicherheit und Grenzen

Kommentiertes Protokoll der Tagung

Andrea Knaut

I. Auftakt – *»ein kurzes schwaches Lob der jetzigen höhern Paßwissenschaft«*[1]

Nur der Pass liefert eine »wahre *Monographie* eines Einzelwesens, auf einem einzigen Folioblatt«. Durch ihn

> »unterscheide z. B. ich mich auswärts von sämtlichen Spitzbuben in der Welt; denn ich zeige meinen gestempelten Papier-Paß vor, worin (außer meiner Handschrift) steht, daß ich 5 Fuß und 10 Zoll lang bin, 59 Jahre alt, in Wunsiedel geboren etc., daß meine Stirn breit und hoch ist und mein Mund klein. Oder läßt es sich nur träumen, daß es gerade einen Spitzbuben geben könnte, auf welchen alles von mir so passete, daß wir einander deckten, wie geometrischgleiche Figuren, oder ineinander eingriffen, wie Kerbhölzer? Unmöglich! – Sogar meine nächsten Nachahmer und Diebe würde mein Paß, so sehr ich auch Swift und Sterne nachgeahmt und bestohlen, auf der Stelle unterscheiden von mir.«[2]

1 Wolfgang Coy beginnt die Tagung mit dem hier zitierten Auszug aus Paul, Jean, 1996: Der Komet. Nikolaus Marggraf. Eine komische Geschichte. In: Sämtliche Werke, Abt. I, Bd. 6, Zweitausendeins, S. 565-1036 (Erstausgabe: Verlag Georg Reimer, 1820-22). Im Internet abrufbar unter: http://gutenberg.spiegel.de/buch/3203/1.

2 Ebd.

Wie wäre Jean Pauls ironische Bewunderung des Ausweisdokuments noch gesteigert worden, hätte es die heute übliche Speicherung der Körpercharakteristika in Form sogenannter biometrischer Merkmale in Pässen und die automatische Personenerkennung schon gegeben. Vielleicht wäre ihm dies als brauchbare Realisierung seines Traums erschienen, dass

> »die Polizei allgemeine Pässe – etwa nach der ersten Beichte – auf den Rücken aller Volljährigen, als zweite Taufscheine, mit Geburtort, Eltern u. s. w. so einbrennen könnte, daß mans mehr sähe als spürte.«[3]

Ein solcher Einfalle zeige nämlich, dass sich

> »ein eingeätztes Paß- oder Flebbenwesen ebensogut mit feinstem Ehrgefühl (trotz allem Anscheine von Brandmarken) vertrage als mit Ersparung von Schreibgebühren, Zeitaufwand und mehr dergleichen.«[4]

Die Biometrie wird oft als Instrument gesehen, den menschlichen Körper selbst zum Ausweis zu machen – eine biopolitisch subtile Brandmarkung also?

Biometrie sei ein Thema, so Coy in seinem Einführungsvortrag, das die Arbeitsgruppe *Informatik in Bildung und Gesellschaft* fast schon immer beschäftigt habe. Nur hätten sich die damit verbundenen Projekte dann doch meist in eine andere Richtung entwickelt, weil es ein sehr schwieriges, ein sehr schlecht greifbares Thema sei. Er nennt es eng verbunden mit dem »Problem der Identität«. Und mit diesem aber ist

3 Ebd.

4 Ebd.

»ein philosophisches Faß ohne Boden aufgemacht: Der Begriff der Identität ist so kompliziert, dass man ihn sicher mit technischen Mitteln leicht lösen kann. Deswegen gibt es die Biometrie, wo zumindest in irgendeiner seltsamen Variante angedeutet wird, man könne Menschen so vermessen, dass sie identifizierbar sind.«

II. »Europäische Biometrie im 19. Jahrhundert: Semiotische Identitäten in Kriminologie und Kriminalistik«[5]

Die Einführung biometrischer Methoden, beginnt Miloš Vec mit seinem Vortrag, hätte um 1900 in der »Wissenschaft […] der Tataufklärung«, der Kriminalistik, »einem semiotischen Geschäft«, einen Bruch mit den bisherigen Praktiken in diesem Bereich dargestellt. Kriminalistinnen sammeln, sichten und interpretieren Zeichen oder Spuren. »Der Kernbereich des Identifizierungsgeschäftes betrifft […] klassischerweise die Aufklärung von Straftaten.« Die Identifizierung von Personen wird allerdings im 19. Jahrhundert zu einem sich verschärfenden Problem, verursacht durch »die Verstädterung, die gestiegene Mobilität der Bevölkerung sowie das Erscheinen des modernen Interventionsstaates«. In diesem lautet das

»Versprechen auf Sicherheit und Wohlstand, zwei Begriffe die Schlüsselmotive aller Staatstheorie und Fluchtpunkt der Zweckbestimmungen sind.«

5 Vortrag von Miloš Vec vom 30.11.12.

Auch die Identitätsfeststellung dient der Sicherheit und dem Wohlstand. Sie verbindet »zivilgesellschaftliche und strafrechtliche, staatliche Interessen«.

Die Liste der Standardinstrumentarien zur Personenerkennung erweitert sich rasant in der zweiten Hälfte des 19. Jahrhunderts: Traditionell gibt es bereits die Steckbriefe, die textuelle Erläuterungen oder Zeichnungen menschlichen Aussehens enthalten und zunächst oft subjektiv und wenig normiert sind. Insbesondere im nachrevolutionieren Frankreich finden Pässe mit genauen Angaben zu Namen, Geschlecht, Alter und Angaben zum Äußeren zunächst Verbreitung. Die Polizeien Europas und der Vereinigten Staaten führen Verbrecheralben mit Personenbeschreibungen ein. Daguerreotypie und Fotografie erweitern diese um Porträtfotos. Aber vor allem treiben die Anthropometrie oder schließlich die Daktyloskopie den Bedeutungszuwachs der kriminaltechnischen Indizienbeweise an. Das Vorverfahren, führt Vec weiter aus, habe bald als reine Stoffsammlung gegolten und die Verdächtige sei ein Beweismittel im eigenen Verfahren geworden. Die Technisierung der Ermittlungsverfahren habe dieses Problem verschärft, und die Kontrolle der Beweisführung sei nach und nach auf die Polizeien übergegangen. Allerdings hätten lange Zeit »Standards und Verfahren der Ermächtigung und der Kontrolle« gefehlt. Ihre »Vergesetzlichung« sei bis zur Jahrhundertwende vom 19. zum 20. Jahrhundert ausgeblieben. Eine Legalisierung der ohnehin schon verwendeten Verfah-

ren des kriminalistischen Erkennungsdienstes habe in Deutschland beispielsweise 1933 mit Paragraph 81b der Strafprozessordnung nachholend stattgefunden.

Insgesamt verliert also vor allem das Beweismittel der Zeugenaussage mit den Entwicklungen des 19. Jahrhunderts im Verhältnis zum »Kronjuwel Sachbeweis« erheblich an Bedeutung. Dieser »Aufstieg des Sachbeweises« und der Bedeutungszuwachs der Wissenschaftszweige Kriminalistik und Kriminologie sei von einem »Rechtfertigungsnarrativ imaginierter Gefahrenpotenziale« begleitet. Es findet eine zunehmende »Verwissenschaftlichung des polizeilichen Erfahrungswissens« mit einer »Obsession [für] terminologische Differenzierung« statt. Ob nun in der Beschreibung besonderer körperlicher Merkmale, der Polizeifotografie, der anthropometrischen Bertillonage oder der Daktyloskopie, es sich lasse im 19. Jahrhundert immer wieder die »Affinität für technokratische Lösungen« als eine Entwicklungslinie erkennen. In dieser Epoche entstehe die zentrale Bedeutung »semiotischer Identität« innerhalb der Kriminalistik, die bis heute auch die Basis digitalisierter Identitätsbeweise innerhalb biometrischer Systeme ist.

> »Identität bezeichnet neben der Übereinstimmung von Sachen insbesondere auch die Vorstellung des äußerlich oder innerlich unveränderlichen Wesenskerns einer Person. Eine Identifizierung vorzunehmen bedeutet die Zuweisung einer Identität zu einem Körper.«

Das bedeutet, wie Vec es später noch etwas anders ausdrückt, dass »erst im Moment der Identifizierung […] eine Konstruktion von Identität stattfindet.«

In der Biometrie wird davon ausgegangen, dass bestimmte unabänderliche, einmalige und universelle Körper- oder Verhaltensmerkmale konstitutiv für eine menschliche Identität sind. Heute werden im Massengebrauch praktisch vor allem Fingerbilder, Gesicht, Iris, Handgeometrie, Stimme oder Hand- bzw. Unterschrift als derartige biometrische Charakteristika genutzt. »Das biometrische Versprechen lautete und lautet bis heute: Die Natur wiederholt sich nicht.« Ironischerweise wiederholt sich auch das Ergebnis einer Messung nicht: Jeder Messvorgang selbst verfälscht das Abbild (Muster) des vermeintlich originalen Charakteristikums stets in einer Weise, dass es nie als dasselbe wiederkehren kann. Die Kunst besteht für die Ingenieurinnen und Programmiererinnen darin, den Messfehler zu minimieren. Könnte es sich also wie schon bei der verheißungsvollen vermeintlich realistischen Fotografie in der Wende zum 20. Jahrhundert erweisen, dass die »Repräsentationen des Identischen« nicht identisch sind oder, schwächer ausgedrückt, dass die genügende »Selbstähnlichkeit« fehlt?

Zumindest bis heute und vermutlich auch in naher Zukunft behält die »Mess-Guerilla« die diskursive Oberhand, vereint in »Fortschrittsoptimismus und männliche[r] Technophilie«.

Die kriminalistischen Methoden sind auch stets als Teil systematischer Erläuterungen in der Ursachen- und Präventionsforschung für kriminelles Verhalten, der Kriminologie, genutzt worden. Vec aber behauptet, der Preis etwa der Daktyloskopie sei der Bedeutungsverlust der mit dem biometrischen Signalement verknüpften »kri-

minogenen Dispositionen […], die Stigmata der Devianz von Lombroso, den Phrenologen und Kriminologen« oder Rassenkundlerinnen. An anderer Stelle weist Vec zwar darauf hin: »Die Anthropometrie hat etwa eine unrühmliche, koloniale Geschichte, in der sie mit der Rassenkunde verbandelt war.« Doch er sieht diese Ausprägungen klar der Vergangenheit zugehörig. Die Hermeneutik in der Kriminologie sei eliminiert worden:

> »Die Zeichen sollten weder auslegungsbedürftig noch kriminologisch auslegungsfähig sein. […] Das biometrische Geschäft hatte den Sinn für die sichtbaren körperlichen Zeichen sozialer, rechtlich relevanter Devianz aufgegeben. Diese leben heute eher in Parawissenschaften, Massenmedien, Physiognomik, Graphologie in hochgradig diskriminierenden Ausformungen fort.«

Doch die Verbannung der kriminogenen Disposition, von der Vec hier spricht, ist nur eine scheinbare. Die Unterstellung der Disposition ist im Gegenteil universell und Voraussetzung für den Gebrauch biometrischer Charakteristiken. Es ändern sich lediglich die Deutungskontexte: Biometrische Erfassung kann beispielsweise auf bestimmte soziale Gruppen beschränkt werden oder Verhalten, Hautfarben, körperliche Dispositionen beabsichtigt oder unbeabsichtigt differenzieren. Dies geschieht weniger nachvollziehbar, und nicht mehr offensichtlich von konkreten Akteuren verantwortet, die weiterhin aufgrund rassistischer, klassistischer oder sexistischer Herrschaftspraktiken diskriminieren. Dessen unbenommen verbinden sich nicht von vornherein bösartige, menschenfeindliche Absichten mit der Forschung an der

Biometrie. Viele Kriminalistinnen oder Informatikerinnen erträumten und erträumen sich mittels Biometrie wissenschaftlich fundiertere Urteile in somit aus ihrer Sicht gerechteren Gerichtsverfahren oder versprechen sich von der sogenannten ‚Anonymen Biometrie' einen verbesserten Persönlichkeitsschutz.

Für Staaten und Obrigkeiten sei das »Identifizierungsgeschäft« nicht nur hinsichtlich der Aufklärung von Straftaten und Ordnungswidrigkeiten oder des Erkennens unbekannter Toter interessant, sondern auch für die Kontrolle der Mobilität bei Ein- und Ausreise und der Teilhabe Einzelner an sozialen Sicherungssystemen.

Auch Privatunternehmen markieren Kundinnen heute mit Ausweisen, Payback-Karten, Armbändchen oder Funk-Chips. Sie erstellen eigene Steckbriefe, in ihrem Jargon: Profile, installieren Kameras und sammeln persönliches Material.

In allen Lebensbereichen lege der »Fokus auf Wiedererkennung« von zur Teilhabe Berechtigten. Dies sei sowohl kulturell durch gesellschaftliche Grundannahmen über »Tätertypen, Bedrohungsszenarien, Gewohnheitsverbrecher« und die damit verbundene kalkulierbare Wiederkehr von Straftaten als auch »technisch induziert«. Im modernen »Präventions- und Prädiktionsstaat« würden zudem »schichtspezifische Verdachtsmomente« institutionalisiert. Das Bürgertum sei zunächst dem Verdacht kriminogener Neigungen entzogen gewesen. Diese »alte Dichotomie« – brave Bürgerinnen und böse Verbrecherinnen – habe bis in die neuere Zeit die »Akzeptanz einer ‚Volksdaktyloskopie'« in manchen Staaten gesenkt. An-

ders verhält es sich dagegen mit der Unique Identification Authority of India (UIDAI) oder der National Database and Registration Authority (NADRA) in Pakistan. Diese Behörden verwalten die größten Biometrie-Datenbanken der Welt, in denen sie sämtliche Staatsbürgerinnen erfassen.

Schließlich konstatiert Vec doch:

> »[Weltweit] keimt erneut der Wunsch auf, naturwissenschaftlich-technisch dennoch etwas über die bösen Neigungen von Individuen zu erfahren. […] Die Vergleichung findet dann […] mit dem Normalfall des unverdächtig Guten statt, von dem aus die physiologische Abweichung zum Verdacht böser Absichten führt. […] Kriminologie und Kriminalistik verhandeln ihr Verhältnis angesichts der aktuellen biometrischen Revolution neu.«

Und so ist es kaum überflüssig, am Ende eine Aussage des Vortrags noch einmal besonders zu hervorzuheben:

> »Identifizierungspflichten sind in einer freiheitlichen Gesellschaft rechtfertigungsbedürftig. Anonymität ist ein mit der Meinungsfreiheit verknüpftes Grundrecht.«

III. »How to liquefy a moving body: Eurodac und die Digitalisierung der Europäischen Grenze«[6]

Die Grenzbiometrie ist Teil der massenhaften Vermessung der Weltbevölkerung zum Zwecke ihrer besseren Kontrollierbarkeit in hoheitlichen Kontexten. Die biome-

6 Vgl. Manuskript des Vortrags vom 30. 11. 12 von Brigitta Kuster und Vassilis Tsianos in diesem Band, Seite 19 (Zitate in diesem Kapitel sind aus selbigem).

trischen Maßnahmen sind dabei in komplexe Regelwerke eingebettet. Eines ist die Dublin-II-Verordnung der Europäischen Union (EU),[7] die das »Regulativ der Mobilität von Nicht-EU-Staatsbürger_innen ohne Visum innerhalb der EU« darstelle, so Brigitta Kuster und Vassilis Tsianos. Das technisches Hilfsmittel dazu, das europäische Fingerabdruckidentifizierungssystem Eurodac, soll absichern, »dass der Mitgliedstaat, der die Einreise eines_r Asylantragssteller_in „verursacht" hat (etwa durch Vergabe eines Visums oder aufgrund mangelnder Sicherung der Grenze), das Asylverfahren durchführen muss.«[8]
Kuster und Tsianos untersuchen in ihrer Forschung diese »digitale Grenze« als soziotechnologisches Objekt. Wenn »Kontrolltechnologien zur Grenzsicherung […nur] in ihren politischen Wirkungen erfasst und kritisiert« werden, blieben die Technologien wie Eurodac zunächst selbst opak und »potenziell funktionstüchtig«. Eine solche Analyse folge »einer Art Blackbox-Epistemologie«. Mit einer ethnografischen »De-Blackboxing-Operation«, die auf die menschliche Konstruktion und Nutzung der

7 Diese Verordnung erfreut sich inzwischen der dritten Überarbeitung. Im Jahr 2003 ersetzte die Dublin-II-Verordnung (EG) Nr. 343/2003 das Dubliner Einkommen von 1990. Seit Mitte 2013 ist die Dublin-III-Verordnung (EG) Nr. 604/2013 in Kraft, weiterhin „zur Festlegung der Kriterien und Verfahren zur Bestimmung des Mitgliedstaats, der für die Prüfung eines von einem Drittstaatsangehörigen oder Staatenlosen in einem Mitgliedstaat gestellten Antrags auf internationalen Schutz zuständig ist".

8 Zu Eurodac siehe Absatz XII.

Informationstechnologie abhebe, lasse sich aber hier auch soziologisch noch weiter gehen.[9]

Die in kategorisierten Mustervergleichen des Identifizierungssystems Eurodac hervorgebrachten Zahlen etablierten, so Kuster und Tsianos, eine »verkörperte Identität der Migration«. Sie würden zu »Bedeutungs- und Legitimationsträgern« für paramilitärische Grenzkontrollaktionen wie die der Rapid Border Intervention Teams (RABIT) an der griechisch-türkischen Evros-Grenze. Dass diese Zahlen alles andere als objektiven Charakter haben, zeigt sich im Interview der beiden Forschenden mit einem Beamten des Bundeskriminalamts (BKA). Der Beamte wundert sich im Gespräch über die Eingabepraxis der Griechen bei der Nutzung von Eurodac und macht einen strategischen Vorschlag, mit welcher Art der Dateneingabe sie »‚viele Asylbewerber loswerden'« könnten.

Doch »Bewegung kommt vor ihrer Kontrolle« – Tsianos und Kuster versuchen zu privilegieren, was eine Grenzkontrolltechnik aus dem Blick verliere: das »Wissen der Migration«, das Wissen der Betroffenen und ihre Erzählungen. In ihren ethnografischen Studien seien sie etwa einem Einwanderer namens Rastaman in der heute von der Polizei zerstörten informellen Siedlung Igoumenitsa begegnet, der davon gesprochen habe, wie er »befragt, fotografiert und ‚gefingert'« wurde. Die mit dem letzten Begriff gemeinte Abnahme der Fingerabdrücke wird so-

9 Ein technisches De-Blackboxing ist auch Aufgabe der ethisch umsichtigen Informatikerin. Siehe dazu den Text von Oepen, Seite 37, bzw. Absatz V für dessen kurze Zusammenfassung sowie die Zusammenfassung des Beitrags von Hansen in Absatz IV.

wohl auf Papier als auch auf einer Glasplatte durchgeführt. Das Glas sei ein Gegenstand, der wiederholt als gefährlich in den migrantischen Geschichten auftauche.

Die Exklusion mittels der digitalen Grenze, die die Migrantinnen nun am Körper trügen, sei, nach Dennis Broeders, zum einen die »*von* der Registrierung bzw. Dokumentation« als Rechtssubjekte und zum anderen die »*durch* Registrierung bzw. Dokumentation« als Rechtlose (Hervorhebung der Autorin). Das Wechselspiel zwischen beiden Formen der Ausgrenzung »bildet Konjunkturen der ‘digital deportability‘ heraus«, die »die Risiken der Mobilität – Geld, Ausdauer, Länge des Unterwegs-Seins und manchmal das Leben selbst« – bedeute. Die »verkörperte Identität der Migration« ist die Summe der »Eurodac-Datenkörper«:

> »Sie machen die mobilen und flüchtigen Körper der Migrant_innen, die sie inskribieren, nicht nur maschinen-lesbar und verifizierbar, sondern auch fluid und hypermobil.[… Migrant_innen tragen] die Grenze zugleich mit sich, wie sie dagegen verstoßen.«

Eine interessante Nebenbemerkung machen Tsianos/Kuster zu einem technischen Aspekt der biometrischen Erkennung: In dem System werden Treffer nach einer sogenannten 1:N-Suche gefunden, bei der ein Muster gegen viele in der Datenbank abgelegte verglichen wird. In der Biometrie wird ein solcher Suchprozess als *Identifizierung* definiert, während eine 1:1-Suche nach hinreichend deckungsähnlichen Mustern als *Verifikation/Authentifikation* bezeichnet wird. Die Autorinnen deuten dies als eine

> »im westlichen (Alltags-)Denken übliche Unterscheidung […] zwischen Wahrheit und Identität. Während die Wahrheit zu erlangen dem Versuch entspricht, die Vermittlung zu liquidieren und auf diese Weise Deckungsgleichheit zu erreichen, ist Identität immer schon konfrontiert mit den Schwierigkeiten des Prozesses, Vielheit abzuziehen. Authentizität wiederum versucht, die Subtraktion der Vielheit der Identität im Singulären anzutreffen.«

Diese schwer zu verstehenden Sätze, die allzu beiläufig in eine Fußnote gesteckt worden sind, thematisieren die kulturelle Verankerung der Verbindung zwischen biometrischen Mustervergleichen und *einer* wahren Identität, in der Vielheit nicht sein darf. Der Text von Herbert Hrachovec in diesem Bändchen vertieft derartige dem Identitätsbegriff zugrundeliegende erkenntnistheoretische Annahmen.[10]

IV. »Biometrie in Zeiten von eIDs, Social Networks und Cloud Computing – die Datenschutzsicht«[11]

Eine informatische Herangehensweise, die der von Tsianos und Kuster beschriebenen Methode des *De-Blackboxing* als Technikdokumentation ähnelt, ist die des Datenschutzes. Diese Perspektive nimmt Marit Hansen ein. Sie erklärt, um das Recht auf informationelle Selbstbestimmung als elementares Schutzrecht des Einzelnen überhaupt aufrechtzuerhalten, »muss jeder natürlich

10 Vgl. Hrachovec, Seite 3, kurz zusammengefasst in Absatz IX.

11 Vortrag von Marit Hansen vom 30.11.12.

auch wissen, was jemand über ihn weiß«. Das erfordere »Transparenz« im Sinne von Verständlichkeit der Technikfunktionalitäten und Auskunftsangebote darüber, sowohl für Laien als auch für Experten. Außerdem müsse »Intervenierbarkeit« sowie die Infragestellung einer datenverarbeitenden Blackbox möglich sein. Ein Individuum dürfe dem System nicht einfach ausgeliefert sein.

Aus Datenschutzsicht sei Biometrie zumeist das »Gegenteil einer Hochsicherheitstechnik«, wozu sie oft verklärt würde. Es gebe viele intransparente Manipulationsmöglichkeiten, beginnend bei der Ersterfassung, dem Enrolment, der Daten, über deren Übertragung bis hin zu deren Abgleich. Vor allem das Prinzip der Intervenierbarkeit sei im Falle eines Systemfehlers kaum gegeben. Auch die lebenslange Bindung der biometrischen Daten an die Person sei hochproblematisch.

Hansen weiß aus ihren Erfahrungen als Mitarbeiterin des Unabhängigen Landeszentrums für Datenschutz in Schleswig-Holstein eine Anekdote über die heimliche und nicht bemerkbare Neukonfiguration eines biometrischen Systems eines Geldautomaten zu berichten. Das System wies häufig fälschlicherweise eigentlich zur Finanztransaktion berechtigte Kundinnen als Identitätsbetrügerinnen ab. Die Bank entschied sich daraufhin, das System kurzfristig derart zu manipulieren, dass es für 24 Stunden einfach jede Kundin als Zugangsberechtigte akzeptierte. Man habe die Folgen, die aus den Beschwerden über die unberechtigten Rückweisungen durch das nicht funktionierende Identifizierungssystem entstan-

den wären, für geschäftsschädigender gehalten als einige wenige mögliche Falschakzeptanzen von unberechtigten Kundinnen. Dieses Beispiel zeigt mehrerlei: Die Betroffene weiß nie, wie der Schwellwert für hinreichende Ähnlichkeit zweier Muster, die ihr den Zugang zu einem durch Biometrie kontrollierten System erlaubt, zu einem bestimmten Zeitpunkt eingestellt ist und bemerkt eine administrative Manipulation dessen nicht. Die Betreiberinnen eines solchen Systems erhalten im Zweifel den Glauben an dessen Funktionieren auch dann aufrecht, wenn sie es außer Kraft setzen. Das können sie, weil es sich um eine Blackbox handelt. Ferner gehen sie, zumindest in diesem kleinen Zeitfenster, davon aus, dass die meisten Kundinnen ohnehin in ehrlicher Absicht nur ihr eigenes Geld abheben möchten.

Ein weiterer besorgniserregender Aspekt sei aus datenschutzrechtlicher Perspektive, dass wesentlich mehr darüber geforscht werde, welche Zusatzinformationen biometrische Daten über bestimmte körperliche oder verhaltensbezogene Dispositionen offenbaren, als dazu, wie sich derartige Zusatzinformationen verbergen und verhindern lassen. Eine potentielle Krankheitserkennung oder das Erkennen einer ethnischen Herkunft mittels Wahrscheinlichkeitsanalysen werde in den gängigen Implementierungen nie prinzipiell ausgeschlossen.

»Bis 5 %, so die Daumenregel«, betrage außerdem der Anteil der Personen, bei denen die gängigen biometrischen Verfahren nicht funktionieren.

Hinzukommen viele weitere Probleme. Beim Reisepass seien retuschierte Fotos einreichbar. Es gebe keine internationalen Standards für die Art der Auswertung der biometrischen Daten an unterschiedlichen Grenzkontrollpunkten. Es würden Rohdaten gespeichert.

All dies sind Belege dafür, wie überstürzt biometrische Systeme im Reiseverkehr eingeführt und auf diese Weise einfach Fakten geschaffen wurden.

Einer der Versuche, Regeln für eine datenschutzsensible Implementierung von biometrischen Systemen zu schaffen, sei die »Stellungnahme 3/2012 zu Entwicklungen im Bereich biometrischer Technologien« der Artikel-29-Datenschutzgruppe der EU vom April 2012.

V. »Transparenz und Datensparsamkeit von elektronischen Ausweisdokumenten in Deutschland«[12]

Exemplarisch für eine zentrale Komponente eines biometrischen Systems sind Ausweisdokumente als Datenträger biometrischer Merkmale. Der Informatiker Dominik Oepen beschäftigt sich in seinem Vortrag mit der Frage der technischen Realisierung des Schutzes der auf den Radio-Frequency-Identification-(RFID-)Chips der Pässe gespeicherten Daten. Diese könnten kontaktlos und damit auch durchaus unbemerkt ausgelesen werden, theoretisch über »Reichweiten von 40 bis 50 Zentimetern«.

12 Vgl. Transkript des Vortrags von Dominik Oepen am 30.11.12 in diesem Band, Seite 37.

Eine bereits »bestehende Kommunikation mit einem Dokument und einem Lesegerät […lässt sich] auch über eine Entfernung von mehreren Metern« belauschen.

»Die Einführung elektronischer Ausweisdokumente in Deutschland erfolgte schrittweise.« Zuvor sei die sogenannte »eCard-Strategie des Bundes« beschlossen worden, um die Verbreitung von Chipkarten »in allen Bereichen von eBusiness und eGoverment« und »vor allem elektronische Authentisierungsdienste und elektronische Signaturdienste« zu fördern. Die eID-Funktion des Ausweises, die etwa Internetgeschäfte sicherer machen soll, sucht man akzeptanzfördernd datensparsam umzusetzen. Dazu gehört beispielsweise, dass für den Zugriff auf Ausweisdaten Zertifikate nötig seien. Diese können Diensteanbieter bei der Vergabestelle für Berechtigungszertifikate erhalten. Sie müssten dazu transparent glaubhaft machen, warum sie welche Daten für ihre Zwecke beim Ausweisinhaber auslesen. Man kann nur »spekulieren, wie gut diese Prüfung tatsächlich erfolgt«. So gebe es, sagt Oepen, »einige Dienste in der freien Wildbahn, wo man sich fragt: Wie sind die denn damit durchgekommen?«

Die eID-Funktion bürokratisiert die in Tauschgeschäften nötigen Vertrauensentscheidungen auf eine unnötige Weise. Zudem ist das Ganze halbherzig umgesetzt: Hoheitliche Systeme wie Grenzterminals sind ausgenommen von der Datensparsamkeitsregelung. Mit ihnen lasse sich auf alle auf dem Ausweischip gespeicherten Daten zugreifen.

Beim elektronischen Aufenthaltstitel wird die neue Qualität der Bürokratisierung durch digitale Systeme ebenfalls deutlich: Die seitens des Staates erforderlichen Aufenthaltstitel seien früher »einfach Aufkleber in den nationalen Reisepässen« gewesen. Nun seien es Chipkarten, die dem Inhaber dieselben Funktionen wie der Personalausweis bieten (oder vielleicht doch: aufzwingen?) und die Abgabe zweier Fingerabdrücke bedingen. Eine vollends kriminalistische Praxis in Kombination mit erhöhter Unsichtbarkeit der Speicherung und des Abrufs von Daten, die ein Ausweisdokument erst zu einem sinnvollen machen, institutionalisieren wohl eher das grundsätzliche Misstrauen einer staatlichen Institution gegenüber einzelnen Individuen.

Wie in der Informatik oft üblich beschreibt Oepen sämtliche Prozesse der nun durch Maschinen gefilterten Zugangskontrollsituation an Grenzen oder bei Geschäften mit personifizierenden Metaphern – es gibt sprachlich keinen Unterschied zwischen Mensch und Maschine:

> »Mit der Chip-Authentication wird die Authentizität des Reisepasses nachgewiesen. Der Reisepass weist also nach, dass es sich um einen echten Pass handelt […] In die andere Richtung weist das Terminal nach, dass es tatsächlich berechtigt ist, auf den Reisepass zuzugreifen. […] Im weiter entwickelten PACE-Protokoll] muss zunächst der Dienstanbieter, bzw. das Inspektionssystem, nachweisen, dass es zum Zugriff auf den Ausweis berechtigt ist, bevor der Ausweis seine Authentizität nachweist.«

Der Anthropomorphismus inspiriert zu verschiedenen Feststellungen zur Durchdringung der IT-Systeme, die ja tatsächlich stets menschliche Interaktionen abbilden und wieder auf diese rückwirken:

Maschinelle Prozesse mit Referenz auf menschliche Aushandlungen zu erklären, macht sie verständlicher – zumindest oberflächlich. Sie appellieren an die alltägliche Erfahrung. Das Ritual, dem Grenzbeamtin und Kontrollierte folgen, ist selbstverständlich bei genauerem Hinsehen ähnlich undurchsichtig wie das maschinelle. Die Handlungsparameter der Beteiligten sind gleichermaßen gekapselt in einer Blackbox. Die Kontrollsituation wird durch das Digitale nun um eine andere Blackbox der elektronischen Übertragungs- und Verschlüsselungsprotokolle erweitert. Sie sind nur oberflächlich einfach zu erklären und hochgradig störbar.

Sie zu manipulieren ist Teil eines technischen Spiels, das sehr ernste Konsequenzen und Motive haben kann. Im Technikjargon gehört die Manipulation menschlicher Interaktion, das *social engineering*, zu einer breiten Palette der sogenannten Angriffsszenarien in IT-Systemen. Dass die Informatik-Systeme komplexe Situationen für Menschen kontrollierbarer machen, ist absurd. Doch ökonomisch ist das Spiel sehr lukrativ. Die Manipulation provoziert die Verbesserung des Manipulierten: Im Spiel mit sich selbst geht am Ende schnell der Blick für Ursache, Wirkung und Sinn einer derart elektronisch stabilisierten Identitätspolitik verloren.

VI. »BeID-Labor«[13]

In technischen Umsetzungen von sogenannten Identitätsnachweisen sind Reflexionen zu ihren historischen, kulturellen oder erkenntnistheoretischen Voraussetzungen nachrangig. Beispielsweise steht die der Biometrie zugrundeliegende Vereinfachung, dass ein Individuum mit Hilfe des Abgleichs von Mustern ein und desselben, bestimmten Anforderungen genügenden Körpermerkmals in allerlei Kontexten und über lange Zeit hinweg wiedererkennbar wäre, kaum zur Debatte. Schließlich sind die sich für das vermeintlich geschlossene technische Biometrie-System stellenden Probleme der Signalverarbeitung, -übertragung, der Effizienz des gesamten Systems und der Mustervergleichsalgorithmen, der Sicherstellung der Datenintegrität und des Schutzes vor Manipulation verzwickt genug.

Genauso aber, wie es unmöglich ist, die Richtigkeit einer automatisierten Personenidentifikation automatisiert zu überprüfen, ist es sinnlos anzunehmen, dass die Biometrie und das Passwesen durch eine immer stärkere Verbesserung der Vergleichsalgorithmen, der Fälschungssicherheit von Ausweisen oder diverser Manipulationserkennungstechniken den gefürchteten Identitätsbetrug vollständig verhindern würden. Die Angst, es in großen Bürokratien, anonymen Städten oder Internetgeschäften mit den Falschen zu tun zu haben, denen zu vertrauen, die man nicht persönlich kennt, ist dennoch der Motor einer Identitätsindustrie und Sicherheitsforschung, die sichere Drittmittel garantieren. Wer

13 Vortrag von Wolf Müller vom 30.11.12.

die Falsche, Kriminelle oder die Angreiferin sein mag, ist historisch, sozial wie räumlich kontextabhängig. Aus Sicht der IT-Sicherheit ist die Angreiferin eine Metapher. Sie bedeutet eine imaginierte Person, die die Integrität und definierte Funktionstüchtigkeit einer datenverarbeitenden Maschine absichtlich stört.

Das *BeID-Labor*, das Wolf Müller vorstellt, steht exemplarisch für die Kooperationen zwischen Forschung, Staat und Industrie. Mit relevanten Ergebnissen der Forschung, »Studien-, Bachelor-, Master-, Diplomarbeiten, Patenten, Papers und Open-Source-Produkten« versorge die Hochschule – in diesem Fall die Humboldt-Universität – via »Industriekontakten« den deutschen Standort mit Technologie. Im Schwung der Innovationsorientierung ist die Verwendung eines bedeutungsgeladenen Begriffs wie *electronic IDentity* nicht mehr als ein Buzzword, das den Drittmittelgebern hingeworfen wird. Die Bereitstellung einer freien Programmierschnittstelle für den elektronischen Personalausweis – eines der zentralen Produkte des BeID-Labors – ist einerseits ein Schritt hinsichtlich dessen technischer Transparenz, andererseits eine Fortschreibung und Vertiefung der staatlichen Kontrolle des Individuums und der diskursiv vorherrschenden Sicherheits- und Präventionslogik.

VII. »Write Me Down, Make Me Real«[14]

Eine Person zu sein bedeutet einen Namen zu haben und von anderen gekannt zu werden. Es findet eine Zuordnung statt. Anonyme Personen sind ein Problem, sie lassen sich nicht zuordnen. In seinem Vortrag unternimmt Christoph Engemann einen geschichtlichen Exkurs zur Bedeutung der Namensgebung und ihrer Sammlung in großen Registern als identitätsstiftende Instrumente.

Die im Mittelalter beginnende Geburtenregistratur der Kirchen habe im Streit der Konfessionen eine »neuartige Verschränkungsstelle von Biomacht und Medien« gebildet: Pastoren seien im 16. Jahrhundert ab dem Konzil von Trient zu Sekretären geworden. »Die Taufe ist ein initialer Schreibakt in der Seele und zugleich auf dem Papier der Kirchenbücher.« Die Zugehörigkeit zur Christenheit werde so manifestiert.

> »Gott […] ist [vor diesem Hintergrund] ein Aufschreibsystem mit unendlicher Speicherkapazität, das die Gesamtheit des Tuns (und Lassens) der Menschen dokumentiert und am Tag des Jüngsten Gerichts abfragt.«

Die katholische Kirche lässt sich als »erste[..] und älteste[..] verfasste biopolitische Bürokratie der westlichen Welt« sehen, in der Geburt und Schreiben in einem »untrennbare[n] Verhältnis« stehen. Allerdings war die Handhabung der Geburtenregistratur bis zu deren Säkularisierung im 18. Jahrhundert wenig strikt. »In protestantischen Regionen fand sie ebenso wenig statt wie in jüdischen Glaubensgemeinschaften.«

14 Vortrag von Christoph Engemann vom 30.11.12.

Neben der Kirche habe auch die spanische Krone im 16. Jahrhundert die Präsenz des Königs in den südamerikanischen Kolonien abgesichert, indem sie von den dortigen Staats- und Kirchenvertretern ein permanentes Beschreiben »alle[r] Dinge und Ereignisse auf der anderen Seite des Atlantik […] – ‚entera noticia de las cosas'« – verlangte. Außerdem würden ab Mitte des 16. Jahrhunderts für jeden nach Nueva Espana eingeschifften Passagier Papiere zur Pflicht. Dies sei für nicht-adlige Menschen ein revolutionärer Schritt gewesen:

> »Plötzlich galten normale Menschen des Schriftlichen würdig, erhielten Urkunden und Dokumente, ein Privileg, das sonst nur Adligen und vielleicht noch anderen wie Richtern zustand. […] Verarbeitet wurden die anfallenden Dokumente in einer zentralen Einrichtung, der 1501 gegründeten Casa de la Contratación in Sevilla.«

Sowohl in der Praxis des »papiernen Königs« in der Kolonisation als auch den Registraturen der Kirchen im Mittelalter drücke sich der Wunsch aus, »die Welt in Schrift umzuwandeln«.

Mit der Französischen Revolution schließlich werde die Geburtenregistratur endgültig säkularisiert, erläutert Engemann.

> »Gleichheit beginnt (…) mit dem unterschiedslos Registriertwerden. […] Im weltlichen Regime der bürgerlichen Gesellschaft ist Bürger sein Geschriebenwerden.«

Die Namen seien dabei »Adressen für die Körper der Individuen«, die zentral sind für deren Regierbarkeit. Sei man ein Mensch ohne derartige Urkunde, Sans Papier, sei

man »nacktes Leben«, dem die »biopolitischen Zuwendungen (oder Zumutungen) […] nicht zuteil werden«. Jeremy Benthams »An Introduction to the Principles of Morals and Legislation« sei Zeugnis einer fundamentalen Verschiebung vom Schreibakt in der Seele zum Schreibakt auf den Körper bis zum 18. Jahrhundert. Bentham nämlich weise auf die Namenstätowierungen der englischen Seeleute hin, um seine Forderung eines für jeden Menschen eindeutigen Namens zu untermauern. Dieser sollte nach seiner Vorstellung dem Individuum durch Registrierung ein Leben lang unauslöschlich zugeschrieben sein, wie eine Tätowierung. Tatsächlich werden in jener Zeit europaweite Verbote willkürlicher Namensänderungen, Zwänge zu eindeutigen Namen hinsichtlich des Geschlechts sowie Einschränkungen im jüdischen Namenssystem durchgesetzt.

> »Geborenwerden ist unter Bedingungen neuzeitlicher Staatlichkeit keineswegs eine selbstverständliche Normalität, sondern ein Medienproblem.«

Engemann berichtet weiter von der Kampagne der Vereinten Nationen zur Verbreitung der Geburtenregistratur in Afrika und Asien: »Write me down, make me real«. Namentlich medial registriert zu sein in einer staatlichen Bürokratie werde hier eng verknüpft mit dem Existenzrecht an sich. Die Kampagne dient der Umsetzung der UN-Kinderrechtskonvention, in der in Artikel 7 die unverzügliche Eintragung jedes Kindes in ein Geburtenregister festgeschrieben ist. Die Kampagne soll beispielsweise Kinderhandel eindämmen oder Bürgerrechte

garantieren. Die Glücksversprechen, die mit einer Identitätsstiftung durch Registrierung verbunden werden, ähneln denen für die Einführung der an biometrische Daten geknüpften eindeutigen Registrierungsnummer Aadhaar durch die bereits oben erwähnte Unique Identification Authority of India (UIDAI). In ihren Werbefilmen propagiert sie nicht weniger als die Lösung des Armutsproblems: Aadhaar soll Zugänge zu staatlichen Leistungen oder zu einem Bankkonto unabhängig von der Kastenzugehörigkeit ermöglichen.

Ein weiterer nicht selten genannter Grund für derartige Registrierungskampagnen ist, dass sie der Namenlosigkeit der Opfer von und Täter in Gewaltverbrechen ein Ende bereite, die bei staatlichen Genoziden ein häufiges Problem im Zusammenhang mit der Straffreiheit der Täter darstellt.

Diese Argumente lassen sich allerdings auch ins genaue Gegenteil verkehren. Der massenhafte systematische Zugriff auf plötzlich unerwünschte Menschengruppen und deren Vernichtung setzt die Verunmöglichung jeglicher Anonymität voraus, wie der Holocaust grausam bewiesen hat.

Die Verwaltung von Namen und Körpern in Registern und damit des Lebens, ist gleichermaßen Bedingung für systematische Massengewaltverbrechen sowie für die Möglichkeit, jemanden dafür zur Verantwortung ziehen zu können. Ein fatales Dilemma der Moderne, das die Unmöglichkeit von Freiheit bedeutet.

Auch die digitale Welt bildet keine Ausnahme. Im Internet werde daher die eindeutige Adressierbarkeit über digitale Signaturen und Registraturen neu erzwungen.

> »Was sich möglicherweise dabei verändert, ist das Verhältnis zwischen Körper, Grenze und Medien: Nicht mehr die Körper kommen zur Grenze und ihren Medien, die Medien kommen als Grenze zum Körper.«

Diese Prognose Engemanns ähnelt den Beobachtungen von Tsianos und Kuster in ihren Ethnografien der digitalen Grenze.

VIII. »Spoofing Biometrics in Science and Fiction – Geschichte(n) wider das unauslöschliche Siegel«[15]

So umfassend individuelle Identität, die staatlich kontrollierbar und verwaltbar ist, auch technisch hergestellt wird: »Das Unterwandern, Hintergehen und Austricksen biometrischer Systeme [ist] überhaupt kein neues Phänomen […]«, schreibt Peter Bittner im Abstract zu seinem Vortrag. Im Gegenteil fänden sich zahlreiche Zeugnisse in Kriminalakten der Polizeien sowie in Filmen und Literatur bereits Anfang des 20. Jahrhunderts.

So seien in den FBI-Akten der 1930er und 1940er Jahre Versuche durch operative Veränderung der Muster, Verbrennung, Abrasion, Verätzung oder Transplantation dokumentiert. Besonders prominent seien die Fälle von John Dillinger oder Gus Winkler.

15 Vortrag von Peter Bittner am 30.11.12.

Mit einem anschaulichen Rückgriff auf eine große Sammlung inspirierender Quellen aus Filmen und Literatur, zurückreichend bis zur »Hightech-Methode zur Herstellung einer Gelatinefolie mit einem „falschen" Fingerabdruck« im Roman »The Red Thumb Mark« aus dem Jahre 1907 von R. Austin Freeman, entwirft Bittner eine »Systematik der Überwindung«: von der Beseitigung und Vermeidung eigener Spuren, über »Elimination oder Veränderung des Merkmalsträgers zur Verschleierung eigener Spuren, die Wiederverwendung vorhandener Spuren« oder über deren Einbettung in einen anderen Kontext, die »Ent-Eignung« oder »Transplantation« fremder Merkmalsträger, bis hin zum Attrappenbau. Auch die Manipulation des biometrischen Systems selbst gehört letztlich dazu.

IX. »Identität ist Spurensuche«[16]

Der philosophische Blick Herbert Hrachovecs eröffnet einen Zugang auf wichtige Bedeutungsdimensionen des Begriffs Identität. Im Sinne der Hermeneutik beinhalte er weniger die »Signifikantengleichheit«, »Identitätsfragen hängen [vielmehr] an Bedeutungsgleichheit«. Am Beispiel von Plagiaten macht der Autor dies schnell anschaulich: Auch ein paraphrasierter Wortlaut kann dasselbe bedeuten bzw. sogar dieselbe Aussage sein. Die »Messbarkeit« dieser Arten von gleicher Bedeutung er-

16 Vortrag von Herbert Hrachovec vom 1.12.12. Ausführlicher findet sich seine Argumentation im gleichnamigen Text dieses Bands, Seite 3.

fordere »Textverständnis«. Beim Wiedererkennen von Personen wiederum finde eine Identitätszuschreibung statt, die auf »Sinneseindrücken und Qualitätszuschreibungen beruht«.

Das in der Philosophie seit hunderten Jahren diskutierte Thema Identität werde bis heute recht unterschiedlich behandelt: Zwei Extreme sind zum einen die »formal-logische Rekonstruktion, […] die No-Nonsense-Identität«, zum anderen »die Please-Let's-Have-Some-Nonsense-Interpretation, das ist die postmoderne Sichtweise«. Bei zweiterer Sichtweise ist laut Derrida »Identität Gleichheit in der Wiederholung«. Identität ist auf Zeitlichkeit verwiesen und »ist eher eine Defensivaktion […] des Etwas-Aufgreifens und -Zugreifens in einem Ablauf, der in dieser Weise nicht gegeben ist.« Die Wiederholung desselben bedürfe »der Variation [und der] Annahme, in der Variation gibt es ein Sich-Durchhaltendes«.

Als logische Formen der Identität würden Reflexivität, Symmetrie und Transitivität gelten. Während tautologische, reflexive Aussagen selbstverständlich identisch seien, gehören symmetrische oder transitive Identitätsaussagen zu denen, »die nicht so sein müssen«. Auch biometrische Identität sei dieser Art. Es müsse gemessen werden. Es handelt sich dann um eine »empirische Identitätsaussage«. Ist es also wahr, dass a=b, dann ist b nichts anderes als a – die Person, auf die b sich bezieht, ist dann dieselbe, auf die a sich bezieht. Die Eigenschaftsbeschreibung eines Begriffes, die Intension, werde hier verwendet, um die Extension, den Umfang des Begriffs, zu bestimmen.

Der Begriff des Messens lasse sich aber sowohl aus dem No-Nonsense- als auch dem Nonsense-Approach darstellen: Es gibt Beobachter, einen beobachteten Prozess und ein Mess-System, das beides verbindet. Nach Bentley sei der Input einer Variable des Systems der »*wahre* Wert« derselben und der Output der gemessene Wert. Die Grundidee ist dabei, dass ein Mess-System verlässlich die Validität eines gemessenen Variablenwerts prüfen kann. Dazu wird ein Maßstab, eine Skala, benötigt.

> »In Hegels Terminologie ergibt der Messvorgang, wie er gewöhnlich verstanden wird, Werte, die *für uns – an sich* sind. Anders gesagt: Wir stellen ein Ergebnis unserer Konstruktion als Ergebnis ohne unsere Konstruktion hin. [Hegel hat in] diesem dialektischen Moment etwas vorgesehen, was eine […] Vorahnung der Dekonstruktion ist, also der Derridaischen postmodernen Zugangsweise: nämlich die Empfehlung, etwas, was man als Position betroffen hat, immer auch zu hinterfragen. […] Der Maßstab steht selbst auf dem Prüfstand.«

Das bringe zwar durchaus »die schöne Auswirkung« einer »Lernbereitschaft« mit sich, die aber auch korrumpieren könne. Dies geschieht, wenn »man den Maßstab dann doch nicht so ernst nimmt und ein bisschen nachkorrigiert aufgrund von Interessen, die man selber hat.«

Hrachovec versöhnt schließlich die formal-logische und die postmoderne Sichtweise auf Identität:

> »Um feststellen zu können, ob zwei Gegebenheiten gleich sind, müssen Umstände gleich bleiben. Umstände sind auf andere Weise „gleich" als Gegebenheiten.«

X. »Bildung zum emanzipatorischen Umgang mit Überwachungstechnologien«[17]

Den Messvorgang zu hinterfragen ist der so wichtige Zweifel, der ein Individuum weniger manipulierbar macht und dessen Fähigkeit, selbständig zu urteilen und klug zu entscheiden, befördert. Weder biometrische Systeme noch irgendeine andere Informationstechnologie sind unfehlbar. Dennoch werden Ausdrücke wie *das Internet*, *der Computer* oder *das IT-System*, die als abstrakte Sammelbegriffe für integrierte, komplexe Techniken stehen, zu Bezeichnungen sakraler Artefakte stilisiert. Sie gelten als Korrektiv des stets als problematisch angeführten menschlichen Versagens und flößen auf dieser Ebene gleichermaßen Furcht ein, denn menschliches Versagen ist aus eigener Erfahrung nachvollziehbarer als maschinelles. Versagen kann eine Sicherheitstechnologie per definitionem nicht. Jede Programmiererin einer Software für die Mustererkennung eines Biometriesystems aber weiß nur allzu gut, auf welch wackligen Füßen die Unfehlbarkeit ihres Programms steht. Die umfassenden Performanzmessungsstandards, komplizierten und selten öffentlich zu findenden konkreten Performanzstudien und halb-offiziellen Wettbewerbe um die besten Algorithmen einzelner Komponenten biometrischer Systeme sprechen Bände. Dennoch sind gerade die permanenten Ausbesserungen der Technologien Antrieb für ihr Wachstum, denn das Misstrauen in herkömmliche Praktiken der Personenidentifikation gepaart mit einem vermeintlich wachsen-

17 Vortrag von Andrea Knaut am 1.12.12.

den Sicherheitsbedarf ist fest in modernen, durch große Apparate verwalteten Organisationen wie Staaten, deren Behörden und großen Konzernen verankert.
Was müssen wir lernen über Biometrie, um ihr Umsichgreifen und dessen Auswirkungen zu begreifen und uns gegen die ihr inhärenten maschinellen Fehlentscheidungen schützen zu können? – Ausgangspunkt der Beantwortung dieser Frage ist, dass ein informatisches System niemals losgelöst von der menschlichen Gesellschaft beurteilt werden kann: Programmierbare Maschinen werden und wurden zur Lösung oder Bearbeitung menschlicher Probleme geschaffen, sie sind auch Projektionen von Wünschen und Hoffnungen. Dementsprechend erschließt sich ein großer Teil des Erfolgs der automatischen Personenerkennung historisch, wie es in einigen hier dokumentierten Vorträgen auch geschehen ist. Gegenwärtige und historische Analysen haben kulturelle, politische und soziale Dimensionen, geben Auskunft über die Machtverhältnisse zwischen zentralen Akteuren, die eine Technologie etablieren und stabilisieren. Im Falle der Biometrie spielen die Polizeien der modernen westlichen Nationalstaaten sowie Militär und Sicherheitsindustrie eine tragende Rolle.

Biometrische Systeme besitzen zahlreiche Angriffsvektoren – sich derer klar bewusst zu sein, verhindert das Ausgeliefertsein und das Ohnmachtsgefühl gegenüber einer solchen Technik. Es muss deutlich werden, dass die Macht der Technik nicht durch sie selbst, sondern durch einen gesamten institutionellen Apparat strukturell entsteht.

Ferner schafft die philosophische Annäherung ein besseres Verständnis für die Denk- bzw. Glaubensmuster, auf denen die moderne Vorstellung menschlicher Identität und ihrer Objektivierung durch Technologie beruht.

Bestandteile einer »Bildung zu einem emanzipatorischen Umgang mit Überwachungstechnologien«, wie es mit dem im Vortrag vorgestellten Schulprojekt getestet wurde, sind:

Erstens, die politische Durchdringung des Zusammenspiels von Sicherheit und Freiheit sowie der Kräfteverhältnisse einzelner Protagonistinnen verschiedener Sicherheitskonzepte, zweitens, die kulturellen Auswirkungen und, drittens, die Ursachen permanenter technologischer Überwachung und software-basierter Auswertung großer Datenmengen digitalisierter menschlicher Spuren. Viertens ist es von großer Bedeutung, die Technik selbst auszuprobieren, zu testen und zu manipulieren, um das praktische Begreifen ihrer Fehler zu ermöglichen. In einem solchen Bildungskonzept ist die komplette Infragestellung von Kontrolltechnologien möglich.

XI. »Verfahren der modernen, technisierten Personenidentifikation: massenhafte biometrische Erfassung«[18]

Das wirtschaftliche Wachstum der Firmen in der Biometrie-Branche seit 2001 stehe direkt mit der staatlichen Förderung in diesem Bereich durch das Bundesministerium des Innern (BMI), das Bundesministerium für Bildung

18 Vortrag von Constanze Kurz vom 1.12.12.

und Forschung (BMBF) oder das Bundesministerium für Wirtschaft und Technologie (BMWi) in Zusammenhang, insbesondere seit der sogenannten „Biometrie-Strategie" der Bundesregierung seit 2005. Ein neueres Projekt im Rahmen dieser Strategie sei, berichtet Constanze Kurz, das Forschungsprojekt DigiDak, unter Beteiligung der Projektgruppe verfassungsverträgliche Technikgestaltung (provet) der Uni Kassel, dessen Ziel »die Erforschung eines automatischen und rechtskonformen Systems zur Sicherung von Fingerabdrücken ist".[19]

Das Wachstum des sicherheitstechnologischen Markts rund um die Biometrie liege über den von Frost & Sullivan in teuren Studien seit 2004 prognostizierten Zahlen – und dies trotz der Biometrie-Studien wie der BioP1- und BioP2-Studie des Bundesamts für Sicherheit in der Informationstechnik (BSI), des BMI und weiterer staatlicher und halbstaatlicher Einrichtungen, mit denen zentrale Argumente für die Verwendung der Fingerabdrücke in Passdokumenten widerlegt wurden. Die Technik habe dort alles andere als zuverlässig funktioniert.

Auch die »Ausweitung der Körpervermessung auf Kinder« für ein biometrisches Gesichtsbild im Kinderreisepass, die sowohl technisch unsinnig als auch ethisch hochbedenklich sei, sei derweil durchgesetzt. Bis heute unternehme die Industrie starke Lobbyarbeit in den Rechts- und Innenausschussanhörungen im Bundestag. Flughäfen seien nach wie vor die größten Abneh-

19 Vgl. Selbstbeschreibung „Bundesministerium für Bildung und Forschung: Digitale Fingerspuren (DigiDak) o. J." http://www.bmbf.de/pubRD/Mustererkennung_D_DigiDak.pdf, 24. 06. 2013.

mer für biometrische Kontrollsysteme. Ein zentrales Verkaufsargument sei hier die Beschleunigung der Grenzkontrolle, faktisch aber verlängerten sich die Zeiten durch ihren Einsatz: »Es sind […] Sicherheitssimulationen, die hier aufgebaut wurden.«

Letztlich sei die Abgabe biometrischer Fingerabdrücke oder Gesichtsbilder für Pässe inzwischen alltäglich. Beim nPA würden inzwischen in ca. 30 Prozent der Fälle sogar freiwillig die Fingerabdrücke abgegeben.

Neuere Entwicklungen seien bspw. Körperscanner, die auch biometrische Technologien integrieren. Der 1000D-Whole-Body-Scanner von Iscon integriere Gesichts- und Iridenerkennung sowie kontaktbehaftete Fingerabdruckerkennung. Diese solle zukünftig aber auch kontaktlos geschehen.

Eine weitere wichtige Entwicklung in diesem Bereich sei die Explosion der DNA-Datenbanken von Straftätern, die im Rahmen des Prümer Vertrags zwischen einzelnen EU-Staaten oder dem Abkommen zur Prävention und Bekämpfung schwerer Kriminalität zwischen den USA und einzelnen EU-Staaten neben anderen Daten ausgetauscht werden – Deutschland ist in beiden Fällen dabei. »DNA-Daten […] werden natürlich wahrgenommen als perfekte biometrische Daten.«

In Großbritannien sei inzwischen ein Fünftel der Männer erfasst. Gerade bei DNA-Daten gibt es sehr

> »wenig Gegenwehr und auch wenig Debatte – [die haben] dieses „Tatort"-Image: genetische Daten sind toll, da[mit] fängt man immer die Täter […]. Für diese Datenbanken wie für alle gilt: Da gibt's eigentlich nur rein, aber nie raus.«

Auch der Consumer-Bereich wird von Kurz angesprochen: Dazu gehören viele verschiedene Anwendungen wie die viel diskutierten Schaufensterpuppen mit Gesichtserkennung, die Anmeldeschnittsstellen an Laptops oder PCs via Gesichtserkennung oder Swipe-Sensoren, Wohnungsschlüssel oder Zündschlüssel. Sehr prominent diskutiert sei auch die Facebook-Gesichtserkennung. Diese sei durch die extrem breite Nutzung hochproblematisch. So würden »sechs Millionen Fotos pro Stunde« auch noch redundant abgelegt. Zwei Drittel der Fotos enthielten laut einer fragwürdigen amerikanischen Studie Gesichter.

Es würden sich jedoch immer wieder Praktiken der Gegenwehr anbieten. Sicherlich sei es sinnvoll, mit entsprechender Bildbearbeitung angepasste biometrische Bilder für die Ausweise abzugeben. Auch Fingerkuppen könnten Behandlungen erfahren, die deren Abgabe erschwert. Prinzipiell sei der europäische Reisepass im übrigen ohne funktionierenden Chip gültig. Bei Nachfragen müsse man standhalten. RFID-Chips könnten mit alten Mikrowellen zerstört werden (1000 Watt sind zu stark, besser 200 Watt, 20 Sekunden Maximum) oder mit sogenannten Zappern, die man selbst bauen könne, aber auch die mechanische Zerstörung durch gezieltes Heraufschlagen mit einem schweren Gegenstand sei vielversprechend.

XII. »EURODAC 2.0? Anmerkungen zur bevorstehenden Öffnung von EURODAC für Strafverfolgungsbehörden aus politikwissenschaftlicher Perspektive«[20]

Die mit der neuen Eurodac-Verordnung[21] ermöglichte Öffnung der Datenbank für den polizeilichen Zugriff stehe wie viele Überwachungstechnologien exemplarisch für den Function Creep einer einmal irgendwie derart etablierten Technologie. Jonathan Aus beantwortet die von ihm aufgeworfene Frage, warum der Zugriff interessant für Polizeien sei, entsprechend knapp:

> »– weil Eurodac mittlerweile zwei Millionen biometrische Datensätze enthält […], einfach, weil es zur Verfügung steht.«

20 Vortrag von Jonathan Aus vom 1.12.12.

21 Verordnung (EU) Nr. 603/2013 des Europäischen Parlaments und des Rates vom 26. Juni 2013 über die Einrichtung von Eurodac für den Abgleich von Fingerabdruckdaten zum Zwecke der effektiven Anwendung der Verordnung (EU) Nr. 604/2013 zur Festlegung der Kriterien und Verfahren zur Bestimmung des Mitgliedstaats, der für die Prüfung eines von einem Drittstaatsangehörigen oder Staatenlosen in einem Mitgliedstaat gestellten Antrags auf internationalen Schutz zuständig ist und über der Gefahrenabwehr und Strafverfolgung dienende Anträge der Gefahrenabwehr- und Strafverfolgungsbehörden der Mitgliedstaaten und Europols auf den Abgleich mit Eurodac-Daten sowie zur Änderung der Verordnung (EU) Nr. 1077/2011 zur Errichtung einer Europäischen Agentur für das Betriebsmanagement von IT-Großsystemen im Raum der Freiheit, der Sicherheit und des Rechts.

Die Frage, ob ein biometrisches Kontrollsystem wie Eurodac dabei wirklich die Lösung eines Problems (»rationalistische Sicht«) ist oder eine Lösung, die nach Problemen sucht (»institutionalistische Sicht«), werfe ein interessantes Licht auf die Art der »Institutionalisierung des ersten AFIS [Automatisiertes Fingerabdruckidentifizierungssystem] auf supranationaler Ebene«. In dieser spielen und spielten zahllose Akteure mit unterschiedlichem Einfluss und unterschiedlichen Interessen eine Rolle. Jonathan Aus hebt besonders das Bundesministerium des Innern oder kommerzielle Anbieter wie Sagem Défense Sécurité (heute Morpho) und das von Steria geführte Konsortium, das auch für das biometrische Visa-Informationssystem und die zweite Generation des Schengener Informationssystems zuständig sei, hervor.

Die zentrale Gesetzesgrundlage für die Etablierung von Eurodac ist, wie oben erwähnt, die sogenannte Dublin-II-Verordnung von 2003. Diese sei kaum im Interesse von EU-Grenzstaaten wie Griechenland oder Italien, die als sogenannte Verursacherstaaten mit Hilfe eines Instruments wie Eurodac viele Illegalisierte aus den Nordstaaten zurücknehmen müssten und dementsprechend wenige illegal Aufgegriffene überhaupt in der Datenbank registrierten. Die Dominanz bestimmter Nationalstaaten innerhalb der EU werde anhand der Asylpolitik sehr deutlich. Die »relative Macht« der einzelnen Staaten verteile sich innerhalb des Geflechts der verschiedenen EU-Institutionen wie u.a. Europäischer Rat, Europäische Kommission, Europäisches Parlament (rechtskonservative Mehrheit), Ministerrat, LIBE Committee, Ratspräsidentschaft,

der Asylum Working Party, den Botschaftern (Comité des représentants permanents) und dem Strategic Committee on Immigration, Frontiers and Asylum (SCIFA). Die langfristige Innen- und Sicherheitspolitik ergebe sich dann jeweils in auf einen bestimmten Zeitraum befristeten Programmen wie aktuell dem Stockholmer Programm, mit dem beispielsweise auch die Verfügbarkeit von Daten in nationalen AFIS oder DNA-Datenbanken sowie deren Austauschbarkeit sichergestellt wird. Es sind darin auch die Koordination von Abschiebeflügen oder militärische Flüchtlingsabwehr vorgesehen. Die systematische Harmonisierung der Migrationskontrolle wird innerhalb der EU verwaltungstechnisch als das Common European Asylum System (CEAS) bezeichnet. All dies bette sich in die sogenannten »internationalen Regime« wie Schengen, G6 oder den Vertrag von Prüm ein.

Bemerkenswert sei in diesem Kontext nicht zuletzt die sogenannte »agencyfication«, mit der die Gründung zahlreicher dezentraler EU-Agenturen per Verordnung bezeichnet wird. Die Agenturen dienen der Vernetzung nationaler Exekutivorgane, wie im Falle der Grenzpolizeien die European Agency for the Management of Operational Cooperation at the External Borders (Frontex). Ein anderes Beispiel ist die European Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (IT Agency), die die Koordination der zahlreichen IT-Überwachungssysteme übernimmt. Inzwischen gibt es dreißig verschiedene solcher agencies. Ihre demokratische Legitimation ist umstritten.

Eurodac ist ein Teil dieses Netzwerks aus Staaten, Industrie, Lobbyorganisationen, Agenturen, Regimen, Abkommen, Verordnungen und IT-Systemen. Es ist ein unmenschliches System für die Betroffenen, die damit für die Nutzung eines eigentlich grundlegenden Menschenrechts auf Bewegungsfreiheit kriminalisiert werden.

> »Ein zunehmendes Problem ist [… die] Selbstverstümmelung […], „voluntary mutilation" oder „wilful alteration" von Fingerkuppen, verätzt oder verbrannt und insofern von Eurodac […] nicht verwertbar. In Frankreich ist das offensichtlich gestiegen von 9% (2005) auf 14% (2011) […] – […] menschenrechtlich betrachtet eine durchaus problematische Tendenz, eine nicht intendierte Nebenfolge.«

Angesichts der erschreckenden Entwicklungen dieser unmenschlichen Politik der entpersonalisierten, automatischen Abweisung scheint eine gewisse Erinnerung vonnöten:

> »Europas historische zivilisatorische Errungenschaft besteht sicherlich nicht darin, dass wir unsere Identität aus der Vermessung unserer Körper gewannen, sondern die Ideen von Menschenrechten und Demokratie zu institutionalisieren wussten.«